Administration Guide

BSG8ew and BSG12aw/ew/tw 1.0

Business Services Gateway

Document Status: **Standard**

Document Number: **NN47928-600**

Document Version: **02.01**

Date: **May 2008**

NORTEL

Copyright © 2008 Nortel Networks, All Rights Reserved

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Document status: Standard

Document version: 02.01

Document date: 14 May 2008

Copyright © 2008, Nortel Networks

All Rights Reserved.

Sourced in Canada and the United States of America

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, NORTEL PROVIDES THIS DOCUMENT “AS-IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. This information and/or products described in this document are subject to change without notice.

Contents

New in this release. 9
Features 9
Security 9
Network Address Translation 10
WiFi support 10
SIP support 10
VoIP gateway 10
IP phone Support 10
Quality of Service 10
Power over Ethernet 10
Ethernet connectivity 10
ADSL interface 10
FXO/FXS ports 11
How to Get Help 13
Getting Help from the Nortel Web site 13
Getting Help over the phone from a Nortel Solutions Center 13
Getting Help from a specialist by using an Express Routing Code 13
Getting Help through a Nortel distributor or reseller 14
Introduction 15
Using the BSG Web UI. 17
Logging on to the BSG 17
Modifying system information 18
Deleting system information 18
BSG security policies 19
Configuring LAN resources 19
Configuring MAC filters 20
Enabling Network Address Translation 22
Configuring dynamic NAT 24
Firewall configuration 25
Defining management access to the BSG 31
Enabling RMON 33
Enabling SSH 34
Configuring authorized clients 35
Configuring remote access 36
Configuring the NAT virtual server 37
Enabling SNMP 38
Configuring SNMP community settings 39

Modifying SNMP community settings 39
Configuring an SNMPv3 user 40
Adding SNMPv3 users to groups 41
Configuring SNMPv3 group privileges 42
Configuring the SNMPv3 view 43
Configuring authorization and authentication 44
Configuring digital certificates 45
Configuring user authentication 46
BSG users and groups 53
Manage users and groups 53
Creating a group 53
Adding privileges to a group 54
Creating a user account 55
Manage passwords 56
Changing a user password 56
Changing the administrator password 57
BSG fault management 59
Configure SNMP alarms and events 59
Enabling alarms and events 59
Configuring SNMP trap settings 60
Viewing T1/E1 alarms 61
Configuring RMON events and alarms 62
Configuring RMON events 62
Configuring RMON alarms 63
BSG performance management 67
Bridge information 67
Viewing bridge information 67
Interface statistics 68
Viewing interface statistics 69
Viewing Ethernet statistics 70
Viewing wireless statistics 71
VLAN Statistics 72
Viewing VLAN FDB Entries 73
Viewing VLAN Multicast Table 73
MSTP Statistics 74
Viewing MSTP information 74
Viewing CIST port statistics 75
Viewing MSTI port statistics 76
RSTP Statistics 77
Viewing RSTP information 77
Viewing RSTP port statistics 78

802.1x statistics 79
Viewing 802.1x port based session statistics 79
Viewing 802.1x MAC based statistics 80
Viewing 802.1x authenticator statistics 81
Viewing 802.1x supplicant statistics 82
Viewing 802.1x MAC session statistics 83
IP Statistics 83
Viewing IP interfaces 83
Viewing ARP Cache 85
Viewing IP Statistics 85
Viewing ICMP Statistics 86
Viewing DHCP Statistics 87
Viewing DHCP binding statistics 87
Viewing DHCP server statistics 88
Viewing DHCP relay statistics 89
Viewing RIP Statistics 89
OSPF Statistics 90
Viewing OSPF statistics 90
Viewing OSPF Interface statistics 91
Viewing VRRP Statistics 92
IGMP Snooping Statistics 93
Viewing IGS V1/V2 statistics 93
Viewing IGS V3 statistics 94
Configuring and viewing RMOM statistics 95
Configuring RMON Ethernet statistics 95
Configuring RMON history 96
Viewing RMON Statistics 97
Viewing NAT statistics 98
Viewing firewall statistics 99
Viewing VPN statistics 100
VPN Statistics 100
VPN IKE Statistics 101
VPN IPSEC Statistics 101
Viewing DSL Line statistics 102
Viewing T1/E1 statistics 103
Viewing T1/E1 current statistics 103
Viewing T1/E1 interval statistics 104
Viewing T1/E1 total statistics 106
SIP Statistics 107
Viewing SIP summary statistics 107
Viewing SIP methods statistics 108
Viewing SIP response statistics 108

Viewing QoS statistics 109
Viewing policer statistics 109
Viewing queue statistics 110
Viewing TACACS statistics 110
BSG system logs 113
Configuring logs 113
Enabling system logging 113
Configuring the syslog IP 114
Configuring e-mail notification 115
Viewing logs 115
Viewing system logs 116
Viewing the VPN log 116
Viewing the firewall log 117
Transferring logs 117
Transferring a log file 117
BSG backup and restore 119
Backing up BSG configuration data 119
Backing up configuration files 119
Restoring the BSG 120
Restoring from a backup file 120
Restoring factory defaults 121
BSG software upgrades 123
Upgrading the BSG software 123
Viewing system information 125
Viewing the system summary 125
Viewing system files 126
Viewing PoE information 127
Viewing the IP interfaces 127
Viewing the Interface status 128
Viewing the DHCP bindings 129
Viewing the ARP cache 130
Viewing the MAC address table 130
Viewing the WLAN stations 131
Common operating procedures 133
Saving configuration files 133
Updating system information 133
Configuring the date and time 135
Rebooting the system 136
Downloading files to the BSG 137
Uploading files from the BSG 138

Initial troubleshooting 139
Network configuration 139
Site network map 139
Logical connections 139
Device configuration information 139
Other important data about your network 140
Normal behavior on your network 140
Useful troubleshooting links 140
Partner Bulletins 141
Knowledge and Solution Engine 141
Using the Knowledge and Solution Engine 141
Diagnostic tools 142
Ping 142
SIP diagnostics 142
T1/E1 loopbacks 143
Advanced troubleshooting on the BSG 145
Switching and routing 146
Layer 2 switching is not functioning 147
Layer 3 forwarding is not functioning 148
LAN host does not receive an automatic IP address 148
WAN and VPN 149
WAN access failure 149
Firewall issues 150
No traffic between WAN and LAN host 151
Verifying site-to-site VPN connectivity 152
DNS does not resolve the domain name 152
PPP link does not start 153
PPP link fails when the WAN interface is DSL 154
Telnet 154
Determining whether Telnet is operational 155
Verifying a Telnet session 155
Determining whether SSH connects 156
BSG subsystem 157
Determining whether VOIP/SafeNet/SIP/ Wireless is operational 157
Troubleshooting SIP 158
Troubleshooting WLAN 164
Firmware upgrade 166

New in this release

The following sections detail what is new in *Administration Guide* for the Business Services Gateway 8-port (BSG) and the BSG 12ew/aw/tw for Release 1.0.

Features

See the following sections for information about feature changes:

- Security
- Network Address Translation
- WiFi support
- SIP support
- VoIP gateway
- IP phone Support
- Quality of Service
- Power over Ethernet
- Ethernet connectivity
- ADSL interface
- FXO/FXS ports

Security

The BSG provides several security features to protect your network.

Stateful firewall

The BSG stateful firewall monitors the connections on all of its interfaces. The BSG uses this monitoring process to filter traffic and to apply security policies established on your network. The stateful firewall also provides protection against port scanning by closing ports until a connection request for a specific port is received.

RADIUS and TACACS authentication

By default, users are authenticated on the local BSG system. Alternately, you can choose to authenticate users on a centralized server using Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS).

VPN with IPSec

Private networking with IPSec ensures that only authorized users can access the network and that data is protected.

Network Address Translation

Network Address Translation (NAT) enables the LAN to use one set of IP addresses for internal traffic and one set of IP addresses for external traffic. This translation allows computers on a private network to access the internet without requiring their own global (public) internet address. The BSG supports three types of NAT: many-to-one, static, and dynamic.

WiFi support

The BSG provides connectivity for an 802.1 WLAN interface.

SIP support

The BSG supports Session Initiated Protocol (SIP) applications. SIP is a signalling protocol for VoIP calls. It is also used for other media types, such as white board sessions and voice-data integration.

VoIP gateway

The BSG provides gateway services for Voice over IP (VoIP) applications, such as the conversion of voice and fax calls between the Public Switched Telephone Network (PSTN) and the IP network.

IP phone Support

The BSG supports IP phones that are connected to your network.

Quality of Service

You can configure and monitor Quality of Service (QoS) levels on your network.

Power over Ethernet

The Power over Ethernet (PoE) ports on the BSG provide power for connected devices. PoE ports help minimize the number of electrical outlets and cables needed at the installation site.

Ethernet connectivity

The BSG provides Ethernet connectivity. The number of Ethernet ports available depends on the model of BSG that you use. The BSG8ew provides 8 ports.

ADSL interface

The BSG12aw provides connections for Asymmetric Digital Subscriber Line (ADSL) equipment.

FXO/FXS ports

The BSG provides connections for Analog Telephony Adapter (ATA), fax, or an analog voice trunk. When you connect an analog voice trunk to the Foreign Exchange Office (FXO) or Foreign Exchange Subsciber (FXS) ports, the analog trunk can be used to connect your network with the PSTN if the digital connections to your ISP fail.

How to Get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchase a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

This guide describes how to manage and maintain BSG 8ew and the BSG 12ew/aw/tw systems.

The concepts, operations, and tasks described in the guide relate to the fault, configuration, performance, and security management features of the BSG system. This guide also describes additional administrative tasks, such as log management, backups, and software updates.

The tasks described in this guide are based on the assumption that you use the BSG with full administrative privileges. If you do not have full administrative privileges, you may see only a subset of the tasks and panels described in this guide.

Navigation

- Using the BSG Web UI (page 17)
- BSG security policies (page 19)
- BSG users and groups (page 53)
- BSG fault management (page 59)
- BSG performance management (page 67)
- BSG system logs (page 113)
- BSG backup and restore (page 119)
- BSG software upgrades (page 123)
- Viewing system information (page 125)
- Common operating procedures (page 133)
- Initial troubleshooting (page 139)
- Advanced troubleshooting on the BSG (page 145)

Using the BSG Web UI

The Web User Interface (Web UI) is the primary management application that you use to configure and administer BSG system. This chapter provides basic procedures for using the Web UI, such as logging in, and modifying and deleting system information.

Navigation

- Logging on to the BSG (page 17)
- Modifying system information (page 18)
- Deleting system information (page 18)

Logging on to the BSG

The Web UI uses standard Internet browsers like Internet Explorer or Firefox to connect to BSG devices over an IP network. Use the following procedure to access the BSG through the Web UI. You can access the Web UI by using any of the following browsers:

- Internet Explorer 6.0
- Internet Explorer 7.0
- Mozilla Firefox

Procedure steps

Step	Action
1	Open the Web browser such as Internet Explorer.
2	In the browser, type the IP address of the BSG.
3	Press **Enter.** The BSG LOGIN page appears.
4	In the **User Name** field, type the user name.
5	In the **Password** field, type the password.
6	Click **Login.** On successful validation of the user name and password, the System Information page appears.

End

Variable definitions

Use the data in the following table to use the fields in the login page.

Variable	Value
User Name	Specifies the user name. The default logon name is nnadmin.
Password	Specifies the password. The default password is PlsChgMe!.

Modifying system information

Many panels on the Web UI have two distinct areas: one area where you can configure new settings, and a second area that lists existing settings in tabular format. For example, on the panel Configuration > System > User Management > Users tab, the area at the top of the screen allows you to enter the information for a new user account, while the table below lists the existing users. When you want to modify an existing setting on the BSG, you can do so using the table provided. Use the following procedure to modify existing system information on the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select the appropriate path for the information that you want to modify**.**
2	In the table, select the row that you want to modify.
3	Modify the settings as needed.
4	Click **Apply.**

End

Deleting system information

Perform the following procedure to delete existing settings on the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select the appropriate path for the information that you want to delete**.**
2	In the table, select the row that you want to delete.
3	Click **Delete.**

End

BSG security policies

You can configure the BSG to apply security to incoming and outgoing traffic on your network. This chapter describes how to configure the system-wide security policies that control network access.

Navigation

- Configuring LAN resources (page 19)
- Defining management access to the BSG (page 31)
- Configuring authorization and authentication (page 44)

Configuring LAN resources

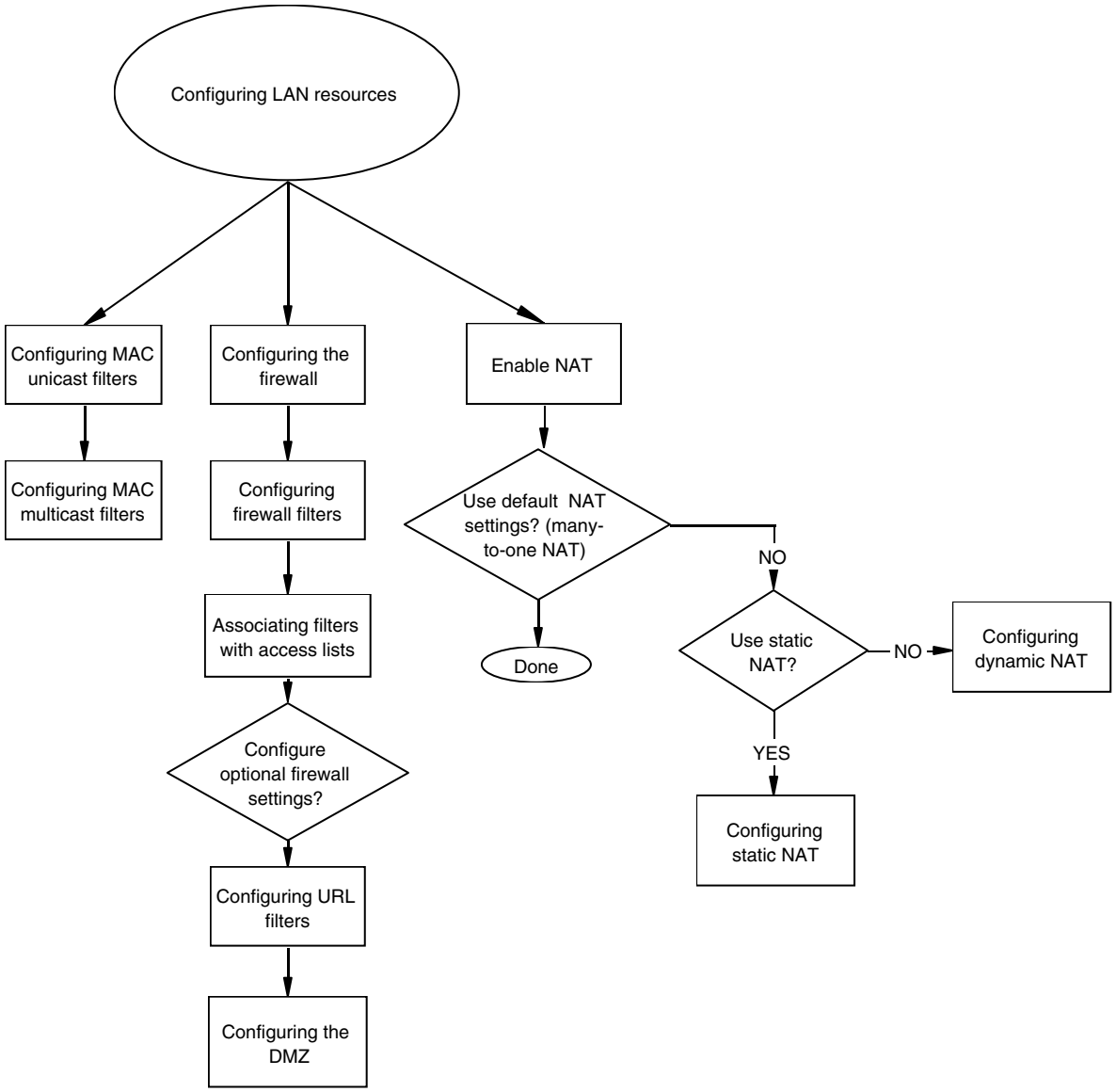
This section provides procedures for configuring the policies that control access to and from the LAN.

Navigation

- Configuring MAC filters (page 20)
- Enabling Network Address Translation (page 22)
- Firewall configuration (page 25)

Use the following flowchart to determine which procedures to perform to define access to the LAN.

Figure 1 Procedures for configuring LAN resources



Configuring MAC filters

This section describes how to configure MAC unicast filters, and MAC multicast filters.

Configuring MAC unicast filters

Use the following procedure to configure Media Access Control (MAC) filters. You can define the MAC addresses of hosts and the LAN ports from which they are allowed to access a configured VLAN on the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Security, MAC Filters**.
	The MAC Filter Configuration dialog box appears.
2	From the **VLAN ID** list, select the VLAN ID.
3	In the **MAC Address** field, type the MAC address.
4	In the **Allowed Ports** field, type the port numbers allowed to access this VLAN.
5	Select a **Status** from the drop-down menu.
6	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the MAC Filter Configuration dialog box.

Variable	Value
VLAN ID	The VLAN ID.
MAC Address	The MAC address.
Allowed Ports	The allowed port range.
Status	The status: Permanent Delete on Reset Delete on Timeout

Configuring MAC multicast filters

Use the following procedure to configure Media Access Control (MAC) filters. The MAC addresses that you configure on this panel are allowed access to your network.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Security, MAC Filters**, **Multicast**.
	The MAC Filter Configuration dialog box appears.
2	From the **VLAN ID** list, select the VLAN ID.
3	In the **MAC Address** field, type the MAC address.
4	In the **Allowed Ports** field, type the port numbers allowed to access this VLAN.
5	In the **Forbidden Ports** field, enter the range of ports that you want to prohibit or prevent from accessing this VLAN.

6 Select a **Status** from the drop-down menu.

7 Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the MAC Filter Configuration dialog box.

Variable	Value
VLAN ID	The VLAN ID.
MAC Address	The MAC address.
Allowed Ports	The allowed port range.
Forbidden Ports	The ports you want to prohibit or prevent.
Status	The status: Permanent Delete on Reset Delete on Timeout

Enabling Network Address Translation

The BSG supports Network Address Translation (NAT). This translation provides security for your LAN by hiding the IP addresses of devices on your network from external computers. The BSG supports many-to-one NAT, static NAT, and dynamic NAT.

Enabling NAT

Use the following procedure to enable NAT on the BSG. When you enable NAT, the system defaults to many-to-one NAT; that is, the BSG translates many administered private IP addresses to a single globally routable IP address.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security, NAT.** The NAT Basic Settings dialog box appears.
2	In the **NAT Status** list, select the status of the NAT as Enabled or Disabled.
3	In the **Idle Time Out (Seconds)** field, type the time to wait before an idle session times out.
4	In the **TCP Time Out (Seconds)** field, type the time to wait before a TCP session times out.
5	In the **UDP Idle Time Out (Seconds)** field, type the time to wait before a UDP session times out.

6 Click **Apply**.

7 Click **Interface Settings** tab.

The NAT Interface Settings dialog box appears.

8 In the **Interface** list, select the interface on which to enable NAT.

9 In the **Address Translation** list, select the status of address translation as enabled or disabled on the interface.

10 In the **Port Translation** list, select the status of the port translation on the interface.

11 Click **Add**.

12 Click **Apply**.

End

Variable definitions

Use the data in the following table to configure the fields in the NAT Basic Settings dialog box.

Variable	Value
NAT status	The status of the NAT as Enabled or Disabled. If you select Enabled, the NAT translation is applied on the incoming and outgoing traffic. If you select Disabled, the NAT translation is not applied on the incoming and outgoing traffic. The default value is Enabled.
Idle Time Out	The number of seconds to elapse before an idle session times out. The configuring values ranges from 60 to 86400 seconds. The default value is 60 seconds.
TCP Time Out	The number of seconds to elapse before a TCP session times out. The configuring values ranges from 300 to 86400 seconds. The default value is 86400 seconds.
UDP Time Out	The number of seconds to elapse before a UDP session times out. The configuring values ranges from 300 to 86400 seconds. The default value is 300 seconds.

Use the data in the following table to configure the fields in the NAT Interface Settings dialog box.

Variable	Value
Interface	The interface on which to configure Network Address Translation and Network Port Translation.

Variable	Value
Address Translation	The status of the Address Translation as Enabled or Disabled. The default value is Enabled.
Port Translation	The status of the Port Translation as Enabled or Disabled. If Port translation status is enabled, then the same global IP address is overloaded and can be used for many local hosts by translating the port number. The default value is Enabled.

Configuring static NAT

Static NAT involves mapping a given local IP address to a unique global IP address. Perform the procedure in this section to configure static NAT.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security**, **NAT.**
2	Click **Static NAT**. The Static NAT dialog box appears.
3	In the **Interface** list, select the interface.
4	In the **Local IP Address** field, type the IP address of the local computer.
5	In the **Translated IP Address** field, type the translated IP address of the local computer.
6	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the Static NAT dialog box.

Variable	Value
Interface	The interface for static NAT configuration.
Local IP Address	The local IP address of the host present in the local network.
Translated Address	The translated IP address used on the Internet.

Configuring dynamic NAT

The dynamic NAT involves mapping the internal IP address to an external IP address, which is drawn from a pool of global IP addresses. The external address varies with each session. When you choose dynamic NAT, you should have the same number of external IP addresses as local IP addresses. Perform the procedure in this section to configure dynamic NAT.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security, NAT.**
2	Click **Dynamic NAT**. The Dynamic NAT dialog box appears.
3	In the **Interface** list, select the interface.
4	In the **Global IP Address Translation** field, type the global IP address.
5	In the **Subnet Mask** field, type the subnet mask.
6	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the dynamic NAT dialog box.

Variable	Value
Interface	Specifies the Interface ID.
Global IP Address	Specifies the global IP address.
Subnet Mask	Specifies the Subnet mask which, combined with the IP address, provides the range of global IP addresses.

Firewall configuration

The BSG stateful firewall monitors the connections on all interfaces. This monitoring process allows the BSG to filter traffic and apply the security policies established in your network. The firewall module blocks all packets that are not explicitly configured to be allowed into the protected network, and provides a logging mechanism to track the IP address and port number of the packets denied by the firewall filtering. The procedures in this section describe how to configure the firewall.

Navigation

- Configuring the firewall (page 25)
- Configuring firewall filters (page 27)
- Configuring the firewall access control list (page 29)
- Configuring the firewall demilitarized zone (page 30)
- Configuring the URL filter (page 31)

Configuring the firewall

Perform the procedure in this section to configure firewall basic settings.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Security, Firewall.**
	The Firewall Basic Settings dialog box appears.
2	In the **Firewall Status** list, select the firewall status as Enabled or Disabled.
3	In the **URL Filtering Status** list, select the URL filtering status as Enabled or Disabled.
4	In the **ICMP Error Generation** list, select the status as Enabled or Disabled.
5	In the **Filter NetBIOS Packets** list, select the status as Enabled or Disabled.
6	In the **Check IP Spoofing** list, select the status as Enabled or Disabled.
7	In the **Examine TCP SYN packets option** list, select the status as Enabled or Disabled.
8	In the **Maximum Filters** field, type the maximum number of filters.
9	In the **Maximum Access-Lists** field, type the maximum number of access lists.
10	In the **Maximum TCP Open Handshaking Count** field, type the number of TCP connection requests entering the firewall module.
11	In the **SYN Time Out (secs)** field, type the time interval after which the TCP connection requests elapse.
12	Click **Apply**.
13	Click the **Interface** tab.
	The Firewall Interface Configuration dialog box appears.
14	In the **Interface** list, select the interface on which to enable the firewall.
15	In the **Type** list, select the type as **Trusted** or **Untrusted**.
16	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the Firewall Basic Settings dialog box.

Variable	Value
Firewall Status	The firewall status: Enabled or Disabled
URL Filtering Status	The URL filtering status: Enabled or Disabled.
ICMP Error Generation	Specifies the ICMP error generation status as Enabled or Disabled. If you select enabled, the BSG will generate and send ICMP error messages. If you select disabled, BSG will not generate and send ICMP error messages.
Filter NetBIOS Packets	Specifies the filter NetBIOS packets status as Enabled or Disabled. If you select enabled, the BSG will drop NetBIOS packets entering the BSG. If you select disabled, the BSG permits NetBIOS packets to be sent.

Variable	Value
Check IP Spoofing	Specifies the check IP spoofing function as enabled or disabled. If you select enabled, the BSG detects and prevents attempts to spoof trusted IP addresses. If you select disabled, the examining of IP spoofing attack is disabled.
Examine TCP SYN packets option	Specifies the the examine TCP SYN packets option as enabled or disabled. If you select enabled, the examining of TCP SYN packets is enabled. If you select disabled, the examining of TCP SYN packets is disabled.
Max Filters	The maximum number of filters allowed. The default value is 100
Max Access-Lists	Displays the maximum number of access lists. The default value is 100.
Maximum TCP Open Handshaking Count	Specifies the number of TCP connection requests entering in the firewall module. The default value is 50.
SYN Time Out (secs)	Specifies the synchronizing timeout value, which represents the time interval after which the TCP connection requests that exceed the threshold are discarded. The default value is 1 second.

Use the data in the following table to configure the fields in the Firewall Interface Configuration dialog box.

Variable	Value
Interface	Specifies the interface ID.
Type	Specifies the type as trusted or untrusted. Trusted indicates a LAN network. Untrusted indicates a WAN network.

Configuring firewall filters

Perform the following procedure to configure firewall filters, which specify the parameters to be checked against the packet.

After you have created firewall filters, you can associate the filters with an access control list. The access control list specifies whether packets that match the configured filter should be permitted or not. See Configuring the firewall access control list (page 29) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security**, **Firewall.**
2	Click **Filters**. The Firewall Filter Configuration dialog box appears.
3	In the **Filter Name** field, type the name of the filter.
4	In the **Source Range** list, select the source range as Any or Subnet.
5	In the **Source Address** field, type the source address.

6 In the **Source Mask** list, select the source mask.

7 In the **Destination Range** list, select the destination range.

8 In the **Destination Address** field, type the destination address.

9 In the **Destination Mask** list, select the destination mask.

10 In the **Protocol** list, select the protocol.

11 In the **Protocol Number** field, type the protocol number.

12 In the **Source Port** field, type the source port.

13 In the **Destination Port** field, type the destination port.

14 Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the Firewall Filter Configuration dialog box.

Variable	Value
Filter Name	Specifies the filter name.
Source Range	Specifies the source range as Any or Subnet.
Source Address	Specifies the source IP address, if you select the source range as Subnet. The default value is 0.0.0.0/0.
Source Mask	Specifies the Source mask, if you select the Source range Subnet.
Destination Range	Specifies the destination range.
Destination Address	Specifies the destination address., if you select the Destination range Subnet.
Destination Mask	Specifies the destination mask, if you select the Destination range Subnet.
Protocol	Specifies the protocol of the incoming packets. Select one of the following options: • Any • ICMP • IGMP • GGP • IP • TCP • EGP • IGP • NVP • UDP • IRTP • IDPR • RSVP • MHRP • IGRP • OSPF • Other

Variable	Value
Protocol Number	Specifies the protocol number. If you set the Protocol list to Any, you do not need to complete this field.
Source Port	Specifies the source port that is to be checked against the packet. The source port value ranges from 1 to 65536.
Destination Port	Specifies the destination port that is to be checked. The destination port value ranges from 1 to 65536.

Configuring the firewall access control list

The Access Control List (ACL) specifies rules that allow or block specific traffic. Use the following procedure to enable and configure the firewall access control list.

Before you configure the access control list, you must create filters. See Configuring firewall filters (page 27) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security, Firewall.**
2	Click **Access List**. The ACL Configuration dialog box appears.
3	In the **ACL Name** field, type the name of the ACL.
4	In the **Filter Name** list, select the filter name.
5	In the **Packet Direction** list, select the direction for the transmission.
6	In the **Action** list, select the action as permit or deny.
7	In the **Priority** field, type the priority of the access rule.
8	In the **Logs** list, select the level of log to generate whenever this ACL is executed.
9	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the ACL Configuration dialog box.

Variable	Value
ACL Name	The name of the new access rule. Maximum 32 characters.
Filter Name	The name of the filter to be associated with the ACL.
Packet Direction	The direction for transmission of packet as trusted to untrusted (outbound packets) and untrusted to trusted (inbound packets).

Variable	Value
Action	The action to be performed for the given access rule as permit or deny. If you select Permit, the packet is permitted if the filter matches. If you select Deny, the packet is rejected and an ICMP message is sent as response.
Priority	The priority value for the access rule, ranging from 1 to 65535. A lower number translates into a higher priority; therefore, and ACL with a priority of 1 will be used over an ACL with a priority of 10 if both ACLs are applicable to a packet.
Logs	Specifies when a packet is permitted or denied. You can select any one from the following options: • None—Firewall logs are not required • Brief—Firewall logs are included in brief • Detail—Firewall logs are included in detail.

Configuring the firewall demilitarized zone

The firewall demillitarized zone (DMZ) allows a computer on the LAN to be exposed on the Internet. It allows the host configured as a DMZ to respond to requests only; the host cannot generate requests. This prevents an attacker from using the DMZ as a launch point to attack other hosts on the LAN. For example, you can use DMZ to allow internet users to access your web server. Use the following procedure to configure the firewall demilitarized zone. You can configure a maximum of 5 DMZ hosts.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security, Firewall.**
2	Click **DMZ**. The DMZ Host Configuration dialog box appears.
3	In the **DMZ Host IP Address**, type the DMZ host IP address.
4	Click **Add**.

End

Variable definitions

Use the data in the following table to configure the fields in the ACL Configuration dialog box.

Variable	Value
DMZ Host IP Address	The IP address of the DMZ host. The host should be located on the LAN side of the BSG.

Configuring the URL filter

Use the following procedure to block access to a specific Unified Resource Locator (URL). When you add a URL filter, the firewall prevents access to that that URL from your network.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Security, Firewall.**
2	Click **URL Filtering.** The URL Filtering Configuration dialog box appears.
3	In the **URL Name** field, type the name of the URL.
4	Click **Add.**

End

Variable definitions

Use the data in the following table to configure the fields in the URL Filtering Configuration dialog box.

Variable	Value
URL Name	Specifies the name of the URL.

Defining management access to the BSG

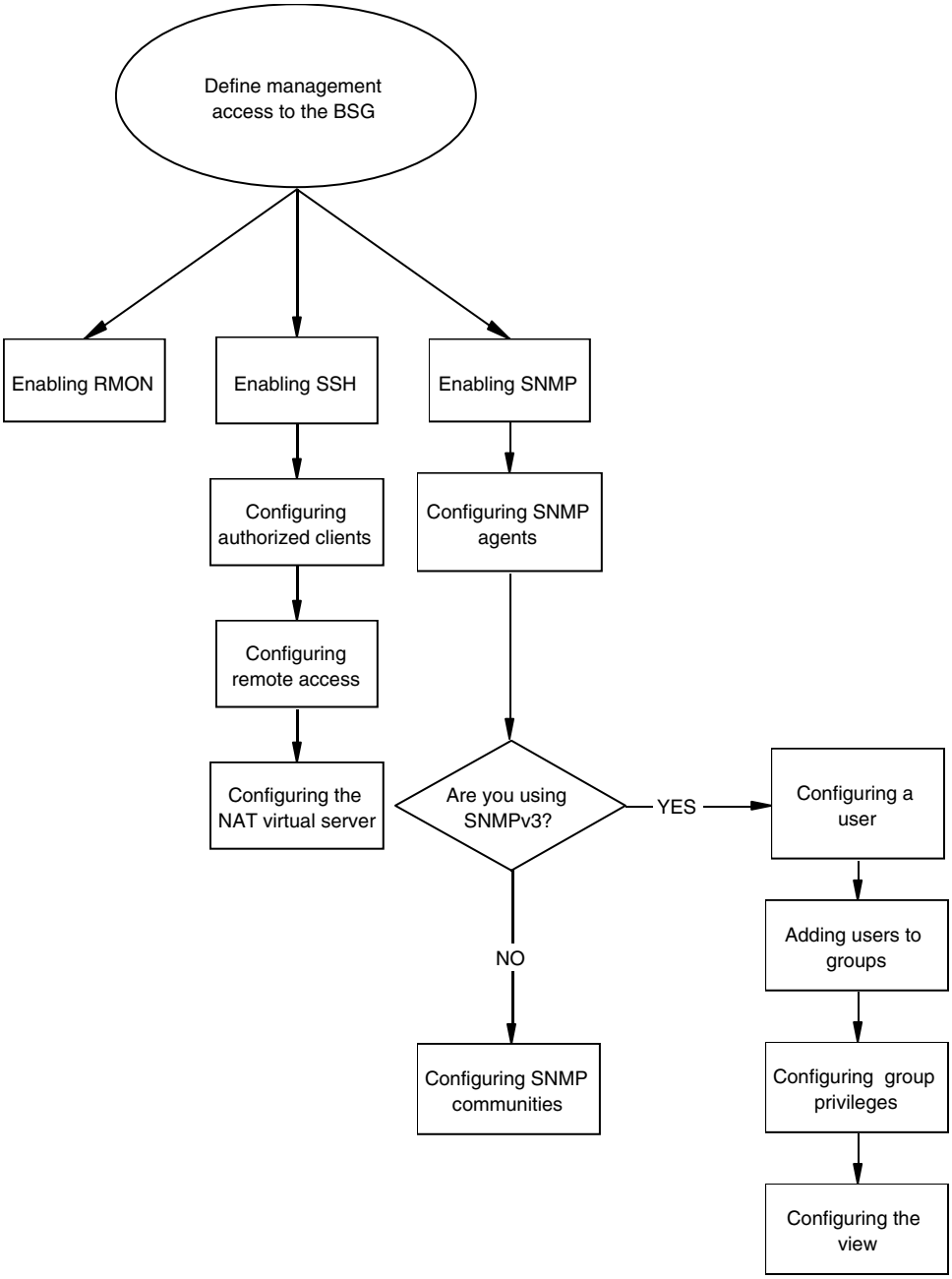
This section provides procedures for configuring how other applications or authorized clients can manage the BSG.

Navigation

- Enabling RMON (page 33)
- Configuring authorized clients (page 35)
- Configuring remote access (page 36)
- Configuring authorized clients (page 35)

- Configuring the NAT virtual server (page 37)
- Enabling SNMP (page 38)
- Configuring SNMP community settings (page 39)
- Modifying SNMP community settings (page 39)
- Configuring an SNMPv3 user (page 40)
- Adding SNMPv3 users to groups (page 41)
- Configuring SNMPv3 group privileges (page 42)
- Configuring the SNMPv3 view (page 43)

Use the following flowchart to determine which procedures you need to complete to configure authorized clients and applications.



Enabling RMON

Use the following procedure to enable RMON. After you enable RMON, you can configure events and alarms; see Configuring RMON events (page 62) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, RMON.**
	The RMON Basic Settings dialog box appears.
2	In the **RMON Status** list, select the RMON status as enabled or disabled.
3	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure basic settings for RMON.

Variable	Value
RMON Status	Specifies the RMON status in the router as enabled or disabled.

Enabling SSH

Use the following procedure to enable SSH so that it can be used for remote managment of the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Device Access.**
2	Click **Authorized Clients.**
	The Authorized Clients dialog box appears.
3	In the **Services Allowed** field, select SSH.
4	Click **Add.**

End

Variable definitions

Use the data in the following table to configure access to authorized clients.

Variable	Value
Services Allowed	Specifies the type of service that is allowed. The following options are available. • ALL—for all types of services. • SNMP—for SNMP based services. • TELNET—for Telnet-based services. • HTTP—for HTTP-based services. • HTTPS—for HTTPS-based services. • SSH—for SSH-based services. The default value is ALL.

Configuring authorized clients

Perform the following procedure to configure access for authorized clients. Authorized clients are those applications that can access and manage the BSG. Access for these clients is based on the IP address of the client.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Device Access.**
2	Click **Authorized Clients.** The Authorized Clients dialog box appears.
3	In the **IP Address** field, type the client IP address.
4	In the **Subnet Mask** field, type the subnet IP address.
5	In the **Port List (Incoming)** field, type the incoming port list.
6	In the **VLANs Allowed** field, type the VLANs that are allowed.
7	In the **Services Allowed** field, choose all the services that are allowed.
8	Click **Add.**

End

Variable definitions

Use the data in the following table to configure access to authorized clients.

Variable	Value
IP Address	Specifies the client IP address.
Subnet Mask	Specifies the subnet mask IP address.

Variable	Value
Port List (Incoming)	Specifies the incoming port list.
VLANs Allowed	Specifies the VLANs which are allowed to access.
Services Allowed	Specifies the type of service that is allowed. The following options are available. • ALL—for all types of services. • SNMP—for SNMP based services. • TELNET—for Telnet-based services. • HTTP—for HTTP-based services. • HTTPS—for HTTPS-based services. • SSH—for SSH-based services. The default value is ALL.

Configuring remote access

Perform the following procedure to configure remote access for the system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Device Access.** The Device Access Settings dialog box appears.
2	Choose the **Allow Telnet Access** check box to access through Telnet.
3	In the **Port** field, type the respective port number.
4	Choose the **Allow Web Access (HTTP)** check box to provide access through the Web.
5	In the **Port** field, type the port number.
6	Select the **Allow Secured Web Access (HTTPS)** check box to provide access through the secured Web.
7	Select the **Allow FTP Access** checkbox to provide access through FTP.
8	In the **Web Inactivity Timeout (secs)** field, type the Web inactive time after which a session terminates.
9	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure remote access to the system.

Variable	Value
Allow Telnet Access	Enables remote to access through Telnet.
Allow Web Access (HTTP)	Enables remote to access through the Web.
Allow Secured Web Access (HTTPS)	Enables remote to access through the secured Web.
Allow FTP Access	Enables remote access through FTP.
Web Inactivity Timeout (secs)	Specifies the inactivity logoff time after which the session logs off automatically, if the device is not accessed for the specified time interval.

Configuring the NAT virtual server

Perform the following procedure to configure the NAT virtual server. When you configure the NAT virtual server, you can manage the BSG from a NAT-enabled interface on the WAN.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **Security**, **NAT.**
2	Click **Virtual Server**.
	The Virtual Server Configuration dialog box appears.
3	In the **Interface** list, select the interface.
4	In the **Local IP Address** field, type the local IP address.
5	In the **Application Type** list, select the type of the application.
6	In the **Local Port Number** field, type the address of the local port.
7	In the **Global Port Number** field, type the address of the global port.
8	In the **Description** field, enter a description of the virtual server.
9	Click **Add.**

End

Variable definitions

Use the data in the following table to configure the fields in the Virtual Server Configuration dialog box.

Variable	Value
Interface	Specifies the Interface ID.
Local IP Address	Specifies the local server IP address located on LAN side.

Variable	Value
Application Type	Specifies the application type for the virtual server. Select the required option for the application of your choice, for example, select ftp to enable FTP on the virtual interface. Select one of the following options: • dns • ftp • pop3 • pptp • smtp • telnet • hhtp • nntp • snmp and • other
Local Port Number	Specifies the local port number if the application type is other.
Global Port Number	Specifies the global port number.
Description	Specifies the description of the virtual server.

Enabling SNMP

Perform the following procedure to enable SNMP.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, SNMP, Basic Settings.** The SNMP Basic Settings dialog box appears.
2	From the **SNMP Agent Status** list, select enable or disable.
3	From the **SNMP Allowed Version** list, select the version.
4	From the **Minimum Security Required** list, select the minimum security required for basic settings.
5	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure the fields in the SNMP basic settings dialog box.

Variable	Value
SNMP Agent Status	Specifies the status of the SNMP agent as Enable or Disable. The default value is Enable.
SNMP Allowed Version	Specifies the operating PDU version of SNMP. Select one of the following options: • V1-V2-V3 - processes V1, v2, and V3 PDUs • V3 - processes only V3 PDUs • V2-V1 - processes V1 and V2 PDUs The default value is V1-V2-V3.
Minimum Security Required	Specifies the minimum security level required for the basic settings. Select one of the following options: • None • Authenticated • Encrypted The default value is None. Authentication and encryption applies only to V3 PDUs.

The Simple Network Management Protocol (SNMP) is commonly used to monitor and manage network devices. This section provides procedures for managing SNMP agents.

Configuring SNMP community settings

Perform the following procedure to configure SNMP community settings if you are using SNMPv1 or SNMPv2 in your network.

Before you begin this procedure, ensure that SNMP is enabled; see Enabling SNMP (page 38) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System**, **SNMP, Community Settings.** The SNMP Community Settings dialog box appears.
2	In the **Community Name** field, type the name of the community.
3	In the **Access Type** list, select the access type as Read-only or Read-write.
4	Click **Add**.

End

Modifying SNMP community settings

Perform the following procedure to modify the settings for SNMPv1 and SNMPv2 communities.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System**, **SNMP, Community Settings.**
2	Choose the option to modify the access type.
3	Click **Apply** to modify the settings, or click **Delete** to delete the selected community.

End

Variable definitions

Use the data in the following procedure to modify the community settings.

Variable	Value
Community Name	Specifies the name of the community. The default name is NETMAN/PUBLIC.
Access Type	Specifies the access type. Select one of the following options. • Read-only • Read-write Set operation fails for a Read-only community.

Configuring an SNMPv3 user

Perform the following procedure to configure SNMPv3 user. Before you begin this procedure, ensure that SNMP is enabled; see Enabling SNMP (page 38) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, SNMP**, **SNMPv3.** The SNMP User Settings dialog box appears.
2	In the **User Name** field, type the user name.
3	In the **Authentication Protocol** field, select the type of the authentication protocol.
4	In the **Authentication Key** field, type the authentication key.
5	Enable the **Encryption Protocol** field to assign the privacy.
6	In the **Encryption Key** field, type the encryption key.
7	Click **Add.**

End

Variable definition

Use the data in the following table to configure SNMPv3 user settings.

Variable	Value
User Name	Specifies the user name. The name is the user-based security-model dependent ID.
Authentication Protocol	Specifies the required authentication protocol. The following options are available. • None—do not authenticate SNMPv3 messages. • MD5—for Message Digest 5-based authentication. • SHA—for Security Hash Algorithm based-authentication.
Authentication Key	Specifies the authentication key, which is the secret key used for messages sent on behalf of the specified user from SNMP.
Encryption Protocol	Enables the encryption protocol to assign the privacy.
Encryption Key	Specifies the encryption key value. Encryption key indicates whether messages sent on behalf of the user from the SNMP are protected from disclosure.

Adding SNMPv3 users to groups

Perform the following procedure to add SNMPv3 users to groups. When you assign users to groups, the group settings define the level of access available for users in the group. Before you begin, ensure that you have configured SNMPv3 groups; see Configuring SNMPv3 group privileges (page 42) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, SNMP, SNMPv3.**
2	Click **Groups.** The SNMP Group Settings dialog box appears.
3	From the **User Name** list, select the user name.
4	In the **Group Name** field, type the name of the group.
5	In the **Storage Type** field, select the type of the storage.
6	Click **Add.**

End

Variable definition

Use the data in the following table to configure SNMPv3 group settings.

Variable	Value
User Name	Specifies the user name.
Group Name	Specifies the group name that is to map to the user. The default value is iso/initial.
Storage Type	Specifies the required storage type for the user-group combination. The following options are available. • Volatile: storage type is temporary; erases configuration settings when the system restarts. • Non-Volatile: storage type is permanent; saves the configuration on the system. You can view the saved configuration when the system restarts.

Configuring SNMPv3 group privileges

Perform the following procedure to configure group access settings for SNMPv3. Group access settings define the level of access available for users in the group. After you use this procedure to define groups and the access level for that group, you can add users to the group; see Adding SNMPv3 users to groups (page 41) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, SNMP, SNMPv3.**
2	Click **Access.** The SNMP Group Access Settings dialog box appears.
3	In the **Group Name** list, select the group name.
4	In the **Security Level** list, select the required security level.
5	In the **Read View** field, type the read view value.
6	In the **Write View** field, type the write view value.
7	In the **Notify View** field, type the notify view value.
8	In the **Storage Type** field, select the type of the storage.
9	Click **Add.**

End

Variable definitions

Use the data in the following table to configure SNMPv3 group access settings.

Variable	Value
Group Name	Specifies the group name that is to map to the user. The default value is iso/initial.
Security Level	Specifies the required security level. The following options are available. • None • Authentication • Encryption
Read View	Specifies the read view value. The group will have read access to this branch.
Write View	Specifies the write view value. The group will have write access to this branch.
Notify View	Specifies the notify view value. The notify view value represents the set of object instances authorized for the group when sending objects in notifications.
Storage Type	Specifies the required storage type for the user-group combination. The following options are available. • Volatile: storage type is temporary; erases configuration settings when the system restarts. • Non-Volatile: storage type is permanent; saves the configuration on the system. You can view the saved configuration when the system restarts.

Configuring the SNMPv3 view

Perform the following procedure to configure view settings for SNMPv3.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, SNMP, SNMPv3.**
2	Click **View.** The SNMP View Settings dialog box appears.
3	In the **View Name** list, select the required view name.
4	In the **Sub Tree** field, type the sub tree value for the view.
5	In the **Mask** field, type the mask value for the view.
6	In the **View Type** list, select the required view type.
7	In the **Storage Type** field, select the type of the storage.
8	Click **Add.**

End

Variable definitions

Use the data in the following table to configure SNMPv3 view settings.

Variable	Value
View Name	Specifies the required view name for which you need to configure view details.
Sub Tree	Specifies the sub tree value for a particular view.
Mask	Specifies the mask value for a particular view.
View Type	Specifies the type of the view. Following options are available. • Included—to allow the sub tree access. • Excluded—to deny the sub tree access.
Notify View	Specifies the notify view value.
Storage Type	Specifies the required storage type for the user-group combination. The following options are available. • Volatile: storage type is temporary; erases configuration settings when the system restarts. • Non-Volatile: storage type is permanent; saves the configuration on the system. You can view the saved configuration when the system restarts.

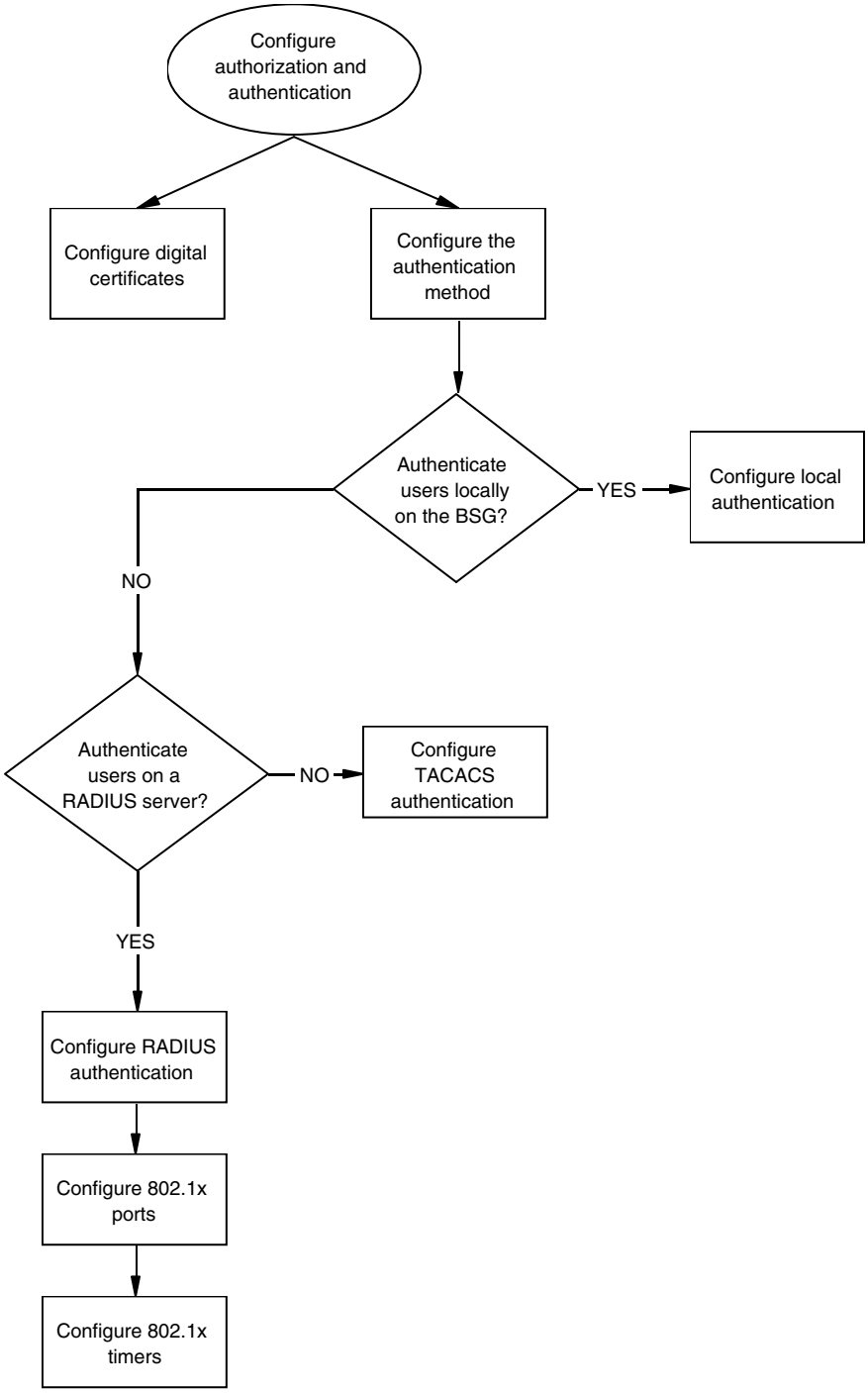
Configuring authorization and authentication

This section provides procedures for configuring how authentication and authorization are handled in your network.

Navigation

- Configuring digital certificates (page 45)
- Configuring user authentication (page 46)

Use the following flowchart to determine which procedures you need to complete to configure authorization and authentication in your network.



Configuring digital certificates

Use the following procedure to determine how digital certificates are issued in your network.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Digital Certificate**.
2	Select the method to use for digital certificates: **Generate Certificate Signing Request**, or **Enter Certificate Signed by Certification Authority**.
3	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure digital certificates.

Variable	Value
Generate Certificate Signing Request	If you enable this variable, you generate a certificate signing request.
RSA Key Size	The RSA key size, in bits. Options: 512 bits 1024 bits
Common Name	The common name of the user.
Enter Certificate Signed By Certification Authority	If you enable this variable, you enter a certificate signed by a certification authority.

Configuring user authentication

The BSG supports options for authenticating users on your network. You can authenticate users locally on the BSG, or you can authenticate users on a RADIUS or TACACS server. This section contains information about how to configure authentication options.

Navigation

- Configuring the authentication method (page 46)
- Configuring TACACS (page 47)
- Configuring RADIUS (page 48)
- Configuring 802.1x ports (page 49)
- Configuring 802.1x timers (page 51)

Configuring the authentication method

Perform the following procedure to configure the method that BSG uses to authenticate users when they access the system. You can configure the BSG to authenticate users on a local database, or users can be authenticated on a RADIUS or TACACS server.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, User Management.** The User Authentication Mode dialog box appears.
2	Select an authentication method: **Radius Authentication**, **TACACS Authentication**, or **Local Authentication**.
3	If you selected Radius authentication, select **Fallback to Local Authentication on RADIUS timeout** to enable local authentication in the event that the Radius server times out or is out of service.
4	If you selected TACACS authentication, select **Fallback to Local Authentication on TACACS timeout** to enable local authentication in the event that the TACACS server times out or is out of service.
5	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure user authentication mode.

Variable	Value
Radius Authentication	Enables the radius authentication.
TACAS Authentication	Enables TACAS authentication.
Local Authentication	Enables the local user name database authentication. This is the default authentication method.
Fallback to Local Authentication on RADIUS timeout	Enables the local authentication when RADIUS fails.
Fallback to Local Authentication on TACACS timeout	Enables the local authentication when TACACS fails.

Configuring TACACS

Terminal Access Controller Access Control System (TACACS) is widely used in network environments. It is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and to authorize their access to the requested system or service. You can configure a mximum of 5 TACACS hosts.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, AAA.** The TACACS Configuration dialog box appears.

2 In the **Server IP Address** field, type the server IP address.

3 In the **Secret Key** field, type the secret key for server authentication.

4 In the **Confirm Secret Key** field, type the secret key again for confirmation.

5 In the **Response Time (Seconds)** field, type the time that the client waits for a response.

6 In the **Single Connection** drop-down menu, select Yes to enable a single connection, or select No to disable a single connection.

7 In the **TCP Port** field, enter the TCP port connected to the TACACS server.

8 Click **Add.**

The server is added to the table below.

9 Select the **Use Server** checkbox if you want to make this server the default authentication server.

End

Variable definitions

Use the data in the following table to configure TACACS.

Variable	Value
Server IP Address	Specifies the server IP address. You can configure a maximum of five TACAS servers.
Secret Key	Specifies the secret authentication key for each server that specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The string length is 64.
Confirm Secret Key	Specifies the secret key.
Response Time (Seconds)	Specifies the time in seconds that a client waits for a response from the server before closing the connection.
Single Connection	Enable a single connection with the TACACS server. Options: Yes No
TCP Port	The TCP port connected to the TACACS server. Maximum 5 characters.
Use Server	When checked, indicates the default server to use for authentication.

Configuring RADIUS

You can use a Remote Authentication Dial-In User Service (RADIUS) server to authenticate users on your network. Use the following procedure to configure the BSG to use RADIUS for user authentication.

When you authenticate users on a RADIUS server, you must also configure the 802.1x port so that the BSG and the RADIUS server can communicate. See Configuring 802.1x ports (page 49) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, AAA.**
2	Click **RADIUS.** The RADIUS Configuration dialog box appears.
3	In the **Server ID** list, select the server ID.
4	In the **IP Address** field, type the IP address of the RADIUS server.
5	In the **Shared Secret** field, type the secret to be shared between the RADIUS server and the client.
6	In the **Response Time (Seconds)** field, type the maximum time within which the RADIUS server must respond to a request from the RADIUS client.
7	In the **Retry Count** field, type the maximum number of times the RADIUS request must be retransmitted.
8	Click **Add.**

End

Variable definitions

Use the data in the following table to configure RADIUS server.

Variable	Value
Server ID	Specifies the server ID, which is a value from 1 to 5.
IP Address	Specifies the IP address of RADIUS server.
Shared Secret	Specifies the shared secret to be shared between the RADIUS server and the RADIUS client. The shared secret is a maximum of 46 characters.
Response Time (Seconds)	Specifies the time in seconds that a RADIUS client waits for a response from the RADIUS server before closing the connection. The value ranges from 1 to 120. The default value is 10 seconds.
Retry Count	Specifies the maximum number of times a RADIUS request is retransmitted before receiving a response from the Radius Server. The value ranges from 1 to 254. The default value is 3.

Configuring 802.1x ports

When you configure the BSG to use RADIUS authentication, or to authenticate devices plugged into the LAN ports of the BSG, you must also configure the 802.1x port. Use the following procedure to configure the 802.1x port.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Port Management, 802.1x.** The 802.1x Basic Settings dialog box appears.
2	In the **802.1x Authentication** list, select the authentication status as enabled or disabled.
3	In the **Authentication Mode** list, select the authentication mode as RADIUS or local.
4	Click **Apply.**
5	Click the **Port Settings** tab**.** The 802.1x Port Settings dialog box appears.
6	In the **Port Control** list, select the port control status.
7	In the **Authentication Mode** list, select the authentication mode as Port based or MAC based**.**
8	In the **Configured Control Direction** list, select the direction.
9	In the **Authentication Retry Count** field, type the maximum authentication requests
10	In the **Re authentication** list, select the reauthentication status as enabled or disabled.
11	In the **Access Control** list, select the authorization state to use when the port is operating as both an authenticator and a supplicant.
12	In the **Max Start** field, type the value currently in use by the supplicant PAE state machine.
13	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure the fields on the Basic Settings panel.

Variable	Value
802.1x Authentication	Specifies the 802.1x authentication status as Enabled or Disabled.
Authentication Mode	Specifies the authentication server mode as Radius or Local.

Use the data in the following table to configure the fields on the Port Settings panel.

Variable	Value
Port ID	Specifies the port name.
Port Control	Specifies the port control value of the port. The following options are available: • ForceUnauthorized • Auto • ForceAuthorized
Authentication Mode	Specifies the authentication mode. The following options are available: • Port based • MAC based You can configure the authentication mode if Port Control is set to Auto.
Configured Control Direction	Specifies the admin control status. The following options are available: • in • both You can configure this setting only if the authentication mode is port based.
Port Status	Specifies the current port status as Authorized or Unauthorized depending upon the connection with the supplicant. Read-only.
Authentication Retry Count	Specifies the maximum number of the authentication requests that are sent from the authenticator before receiving a response from the supplicant. The value ranges from 1 to 10.
Re authentication	Specifies the reauthentication status as enabled or disabled. The default value is Disabled. Reauthentication is enabled only if the port control status for the port is auto.
Access Control	The authorization state when the port is operating as both a supplicant and an authenticator.
Max Start	The maximum number of EAPOL-Start messages that are sent by the supplicant if no response is received.

Configuring 802.1x timers

Use the following procedure to set the timeout value for the 802.1x port. The default values are normally sufficient for most networks; however, you can change the value if a longer timeout is needed.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Port Management, 802.1x.**
2	Click **Timers.** The 802.1x Timer Configuration dialog box appears.

3 In the **Port** field, type the port name.

4 In the **Quiet Period (Seconds)** field, type the period that the authenticator is silent.

5 In the **Transmit Period (Seconds)** field, type the period that the authenticator state machine is used.

6 In the **Supplicant Timeout (Seconds)** field, type the supplicant timeout value.

7 In the **Server Timeout (Seconds)** field, type the server timeout value.

8 In the **Re-authentication Period (Seconds)** field, type the time between the periodic reauthentication of the supplicant.

9 Click **Apply.**

End

Variable definitions

Use the data in the following table to configure timers for 802.1x.

Variable	Value
Port	Specifies the port name.
Quiet Period (Seconds)	Specifies the time that the authenticator is silent and cannot attempt to acquire supplicant.
Transmit Period (Seconds)	Specifies the time that the authenticator state machine uses to define when you need to transmit EAPOL PDU. The default value is 30 seconds. The value ranges from 1 to 65535.
Supplicant Timeout (Seconds)	Specifies the supplicant timeout value.
Server Timeout (Seconds)	Specifies the server timeout value.
Re-authentication Period (Seconds)	Specifies the time between the periodic reauthentication of the supplicant. The default value is 3600 seconds. The value ranges from 1 to 65535.

BSG users and groups

This chapter provides procedures for configuring the users and groups that have access to the BSG. You can use the information in this chapter to manage user accounts, groups and privileges, and passwords.

Navigation

- "Manage users and groups" (page 53)
- “Manage passwords” on page 56

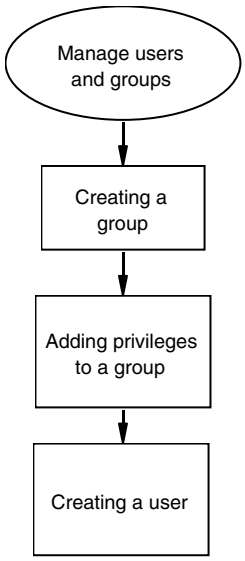
Manage users and groups

This section provides procedures for managing users and groups.

Navigation

- Creating a group (page 53)
- Adding privileges to a group (page 54)
- Creating a user account (page 55)

The following flowchart lists the procedures you need to manage user groups in your network.



Creating a group

Perform the following procedure to configure a group.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, User Management.**
2	Click **Groups.** The Groups Management dialog box appears.
3	In the **Group Name** field, type the group name.
4	In the **Functional Group Access** list, select the required group access.
5	Click **ADD** to add a particular group access from the list. The selected entry appears in the **Functional Group Access for Group.**
6	Select an entry in the **Functional Group Access for Group** and click **REMOVE** to delete a particular group access from the list.
7	Click **Create Group** to create a group with the selected functional group access details.

End

Variable definitions

Use the data in the following table to configure group management details.

Variable	Value
Group Name	Specifies the name of the group.
Functional Group Access	Specifies the list of available functional group accesses. Select a particular access and click Add to add in to a functional group access for group list.
Functional Group Access for Group	Specifies the functional group access configured for a particular group. To remove access from a group, select the required entry, and click Remove.

Adding privileges to a group

Perform the following procedure to add privileges to a group.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, User Management.**

2 Click **Groups.**

The Groups Management dialog box appears.

3 In the **Group Name** field, type the group name.

4 In the **Functional Group Access** list, select the required group access.

5 Click **ADD** to add a particular group access from the list. The selected entry appears in the **Functional Group Access for Group.**

6 Select an entry in the **Functional Group Access for Group** and click **REMOVE** to delete a particular group access from the list.

7 Click **Create Group** to create a group with the selected functional group access details.

End

Variable definitions

Use the data in the following table to configure group management details.

Variable	Value
Group Name	Specifies the name of the group.
Functional Group Access	Specifies the list of available functional group accesses. Select a particular access and click Add to add in to a functional group access for group list.
Functional Group Access for Group	Specifies the functional group access configured for a particular group. To remove access from a group, select the required entry, and click Remove.

Creating a user account

Perform the following procedure to create a user account. You add users to groups when yoiu create the account.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, User Management.**
2	Click **Users.** The User Management dialog box appears.
3	In the **User Name** field, type the user name.

4 In the **Password** field, type the password.

5 In the **Confirm Password** field, type the password again.

6 In the **Group** field, type the name of the group to which the user belongs.

7 Click **Add.**

End

Variable definitions

Use the data in the following table to configure user management dialog box.

Variable	Value
User Name	Specifies the name of the user.
Password	Specifies the password.
Confirm Password	Specifies the password.
Group	Specifies the group name to which the user belongs to.

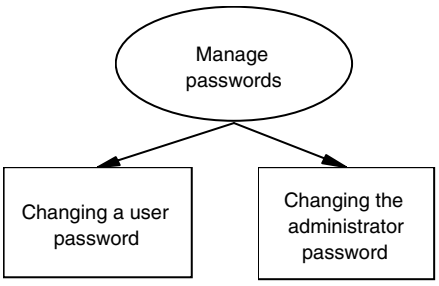
Manage passwords

This section provides procedures for managing passwords.

Navigation

- "Changing a user password" (page 56)
- Changing the administrator password (page 57)

The following flowchart lists the procedures you need to manage user accounts in your network.



Changing a user password

Use the following procedure to change a user's password.

Procedure steps

Step Action

1 From the BSG navigation panel, select **Configuration, System, User Management.**

2 Click **Users.**

The User Management dialog box appears.

3 In the table, select the radio button next to the name of the user whose password you want to change.

4 Select the **Change Password** checkbox.

5 In the **Password** field, type the new password.

6 Click **Apply.**

End

Variable definitions

Use the data in the following table to configure user management dialog box.

Variable	Value
User Name	Specifies the name of the user.
Password	Specifies the password.
Confirm Password	Specifies the password.
Group	Specifies the group name to which the user belongs to.

Changing the administrator password

Perform the following procedure to configure the administration password. To change the password, the change password option in the User Configuration dialog box must be enabled.

Procedure steps

Step Action

1 From the BSG navigation panel, select **Configuration, System, User Management.**

2 Click the **Users** tab**.**

The User Management dialog box appears.

3 In the table, select the radio button next to the administrator account.

4 Select the **Change Password** checkbox.

5 Click **Apply.**

6 Click the **Administrators** tab**.**

The Administration Password dialog box appears.

7 In the **Old Password** field, type the previous password.

8 In the **New Password** field, type the new password.

9 In the **Confirm Password** field, type the password again.

10 Click **Apply.**

End

Variable definitions

Use the data in the following table to configure administration password.

Variable	Value
Old Password	Specifies the old password.
New Password	Specifies the new password.
Confirm Password	Specifies the new password.

BSG fault management

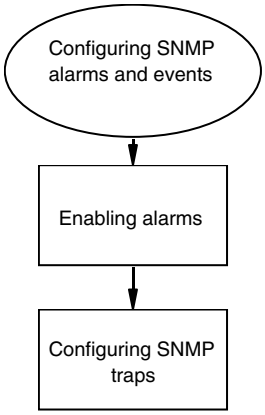
This chapter provides information about how to configure alarms and events on the BSG.

Navigation

- Configure SNMP alarms and events (page 59)
- Viewing T1/E1 alarms (page 61)
- Configuring RMON events and alarms (page 62)

Configure SNMP alarms and events

The procedures in this section describe how to enable SNMP alarms and events and configure trap settings.



Enabling alarms and events

Use this procedure to specify the SNMP traps to be generated. The BSG generates corresponding logs and saves them in the system log whenever a trap is generated. For information about how to access system logs, see Viewing system logs (page 116).

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Alarms.** The Alarms dialog box appears.
2	Select the alarms and events that you want to record in the system log.
3	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure alarms.

Variable	Value
Cold Start	Generates an alarm when the system undergoes a cold start.
Interface Link Status Change	Generates an alarm when the interface link status changes.
Dsx1 Line Status Change (T1/E1 Carrier)	Generates an alarm when a configured DSx interface changes status.
SIP Server Status Change and Configuration Change	Generates an alarm when the SIP server status changes and configuration changes.
PoE Power Notification	Generates an alarm when power turns on or off.
DHCP Pool Limit	Generates an alarm when the DHCP pool limit is reached.
Firewall Attack	Generates an alarm when firewall attacks occur.

Configuring SNMP trap settings

Perform the following procedure to configure SNMP trap settings.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration**, **System, SNMP**, **Traps.** The SNMP Trap Settings dialog box appears.
2	In the **Manager Name** field, type the name of the SNMP manager.
3	In the **Manager Address** field, type the IP address of the SNMP manager.
4	In the **SNMP Version** list, select the required SNMP version.
5	In the **Notify Name** list, select the community name.
6	In the **User Name** list, select the user name.
7	In the **Security Level** field, select the required security level.
8	In the **Trap Type** field, select the required notification type.
9	In the **INFORM Retransmit Interval** field, type the retransmit time interval.
10	In the **INFORM Retransmit Count** field, type the retransmit count.
11	Click **Add**.

End

Variable definitions

Use the data in the following procedure to configure trap settings.

Variable	Value
Manager Name	Specifies the name of the SNMP manager.
Manager Address	Specifies the IP address of the destination where the SNMP traps are to be sent.
SNMP Version	Specifies the required SNMP version. The following options are available. • V1/V2c—specifies the SNMP version 1 and 2. • V3—specifies the SNMP version 3.
Notify Name	Specifies the community name. This is disabled when SNMP version is V3.
User Name	Specifies the user name. This field is disabled when SNMP version is V1/V2c.
Security Level	Specifies the required security level. The following options are available. • None • Authenticated • Encrypted This field is disabled when SNMP version is V1/V2c.
Trap Type	Specifies the required notification type.The following options are available. • Inform—specifies that the message contains InfoRequest PDUs. • Trap—specifies that the message contains snmpv2-trap PDUs.
INFORM Retransmit Interval	Specifies the retransmit interval. It is disabled if the trap type is trap.
INFORM Retransmit Count	Specifies the retransmit count. It is disabled if the trap type is trap.

Viewing T1/E1 alarms

Use this procedure to view the alarm status on T1/E1 connections on the BSG12tw.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, WAN, T1/E1, Alarms.** The Alarm Status dialog box appears.
2	Click **Refresh** to view the current status.

End

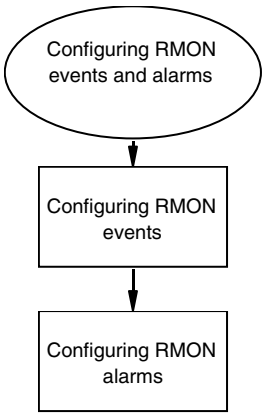
Variable definitions

Use the data in the following table to review the status of alarms on T1/E1 connections.

Variable	Value
Interface	The T1/E1 controller.
No Alarm	When the indicator is green, the T1/E1 link is in-service and no alarm conditions exist.
Yellow Alarm	When the indicator is yellow, there is a far-end loss of frame (LOF) error.
Red Alarm	When the indicator is red, there is a near-end loss of frame (LOF) error.

Configuring RMON events and alarms

The procedures in this section describe how to configure RMON events, and then configure alarms associated with those events.



Configuring RMON events

Use the following procedure to configure events for RMON. Before you begin, ensure that RMON is enabled; see Enabling RMON (page 33) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, RMON.**
2	Click **Events.**
	The Event Configuration dialog box appears.
3	In the **Event Index** field, type the RMON event index number.
4	In the **Description** field, type the brief description about an event.

5 In the **Type** list, select the type of event to configure.

6 In the **Community** field, type the SNMP community used.

7 In the **Owner** field, type the owner name of the event.

8 Click **Add.**

The event displays in the table below.

9 Select the radio button next to the event, and from the **Status** drop-down menu, select a status for the event.

10 Click **Apply**.

End

Variable definitions

Use the data in the following table to configure events for RMON.

Variable	Value
Event Index	Specifies the event index for the RMON events table. It is a number that uniquely identifies an entry in the Events table. Each entry defines one event that is to be generated when appropriate conditions occur. The configuring values range from 1 to 65535.
Description	Specifies the brief description of the event. The display string ranges from 0 to 127 characters.
Type	Specifies the type of event to be configured. The following options are available: • None • Log—an entry is created in the log table for each event. • SNMP Trap—an SNMP trap is sent to one or more management stations. • Log and Trap
Community	Specifies the SNMP community string used for this trap, if the SNMP trap or Log and Trap is selected.
Owner	Specifies the name of the owner of that event. The owner represents the entity that configured this entry and is using the resources assigned to it.
Status	Specifies the status of the event: Valid Invalid Under Creation

Configuring RMON alarms

Use the following procedure to configure alarms for RMON. Before you configure alarms for RMON, you must configure RMON events; see Configuring RMON events (page 62) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, RMON.**
2	Click **Alarms.** The RMON Alarm Configuration dialog box appears.
3	In the **Index** field, type the RMON alarm table index number.
4	In the **Interval** field, type the time interval for which the alarm monitors variable.
5	In the **Variable** list, select the MIB object variable on which the alarm is configured.
6	In the **Sample Type** list, select the type of the sample as absolute value or delta value.
7	In the **Rising Threshold** field, type the rising threshold value.
8	In the **Falling Threshold** field, type the falling threshold value.
9	In the **Rising Event Index** list, select the rising event index.
10	In the **Falling Event Index** list, select the falling event index.
11	In the **Owner** field, type the name of the event owner.
12	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure alarms for RMON.

Variable	Value
Index	Specifies the RMON alarm table index, which uniquely identifies an entry in the alarm table. The value ranges from 1 to 65535.
Interval	Specifies the time interval in seconds for which the alarm monitors the variable. During this interval, the data is sampled and compared with the rising and falling thresholds.
Variable	Specifies the MIB object variable on which the alarm is configured.
Sample Type	Specifies the sample type as absolute value or delta value. If you select Absolute value, then the value of the selected variable is directly compared with the thresholds at the end of the sampling interval. If you select Delta value, then the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Rising Threshold	Specifies the rising threshold value, when the alarm is configured as rising alarm. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.

Variable	Value
Falling Threshold	Specifies the falling threshold value, when the alarm is set as falling alarm. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event Index	Specifies the rising event index, which is raised when the rising threshold is reached.
Falling Event Index	Specifies the falling event index, which is raised when the falling threshold is reached.
Owner	Specifies the owner of the alarm. The owner represents the entity that configured this entry and is using the resources assigned to it.

BSG performance management

You can view detailed information about the performance of the BSG system. This chapter describes information about how to monitor BSG performance information.

Navigation

- Bridge information (page 67)
- Interface statistics (page 68)
- Viewing wireless statistics (page 71)
- VLAN Statistics (page 72)
- MSTP Statistics (page 74)
- RSTP Statistics (page 77)
- 802.1x statistics (page 79)
- IP Statistics (page 83)
- Viewing DHCP Statistics (page 87)
- Viewing RIP Statistics (page 89)
- OSPF Statistics (page 90)
- Viewing VRRP Statistics (page 92)
- IGMP Snooping Statistics (page 93)
- Configuring and viewing RMOM statistics (page 95)
- Viewing NAT statistics (page 98)
- Viewing firewall statistics (page 99)
- Viewing VPN statistics (page 100)
- Viewing DSL Line statistics (page 102)
- Viewing T1/E1 statistics (page 103)
- SIP Statistics (page 107)
- Viewing QoS statistics (page 109)
- Viewing TACACS statistics (page 110)

Bridge information

This section provides information about how to view bridge and spanning tree information.

Viewing bridge information

Use the following procedure to view bridge information for the BSG system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Spanning Tree.**
	The Bridge Information dialog box appears.
	End

Variable definitions

Use the data in the following table to view the bridge information of BSG.

Variable	Value
Address	The MAC address of the bridge.
Bridge Status	The bridge status.
Protocol Specification	The protocol specification.
Priority	The bridge priority.
Time since Topology Change	The time since the topology has changed.
Topology Changes	The number of topology changes.
Transmit Hold-Count	The transmit hold count.
Designated Root	The designated root.
Root Cost	The root cost.
Root Port	The root port.
Max Age (Seconds)	The maximum age.
Hello Time (Seconds)	Specifies the hello time.
Hold Time (Seconds)	The hold time.
Forward Delay (Seconds)	The forward delay time.
Bridge Max Age (Seconds)	The maximum age of the bridge.
Bridge Hello Time (Seconds)	The hello time of the bridge.
Bridge Forward Delay (Seconds)	The forward delay time of the bridge.

Interface statistics

Use the following procedures to view the interface statistics.

Navigation

- Viewing interface statistics (page 69)
- Viewing Ethernet statistics (page 70)

Viewing interface statistics

Use the following procedure to view the interface statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, Interface**. The Interface Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Interface Statistics page.

Variable	Value
Port	The configuring port.
Port Name	The port name.
MTU	The Maximum Transmission Unit (MTU) of the port.
Speed (Bits Per Second)	The current bandwidth of the interface measured in bits per second.
Received Octets	The total number of octets with framing characters received on the interface.
Received Unicast Packets	The number of packets delivered by a sublayer to a higher sublayer. These packets are not addressed to a multicast or broadcast address at this sublayer.
Received Multicast Packets	The number of packets delivered by a sublayer to a higher sublayer. These packets are addressed to a multicast or broadcast address at this sublayer.
Received Discards	The number of inbound packets without errors that are not delivered to a higher-level protocol.
Received Errors	In a packet-oriented interfaces, the number of inbound packets with errors that are not delivered to a higher-layer protocol. In a character-oriented interface or fixed-length interface, the number of inbound transmission units with errors that are not delivered to a higher-layer protocol.

Variable	Value
Received Unknown Protocols	For a packet-oriented interface, the number of packets which are discarded because of an unknown or unsupported protocol. For a character-oriented interface or fixed-length interface, the number of transmission units received that are discarded because of an unknown or unsupported protocol. For an interface that does not support protocol multiplexing, this counter will always be 0.
Transmitted Octets	The total number of octets with framing characters transmitted from the interface.
Transmitted Unicast Packets	The number of packets transmitted by a sublayer to a higher sublayer. These packets are not addressed to a multicast or broadcast address at this sublayer. This number includes the discarded packets.
Transmitted Multicast Packets	The number of packets transmitted by a sublayer to a higher-level protocol. These packets are addressed to a multicast or broadcast address at this sublayer.
Transmitted Discards	The number of inbound packets without errors which are not transmitted to a higher-level protocol.
Transmitted Errors	In a packet-oriented interfaces, the number of outbound packets with errors which are not transmitted to a higher-layer protocol. In a character-oriented interface or fixed-length interface, the number of outbound transmission units with errors which are not delivered to a higher-layer protocol.

Viewing Ethernet statistics

Use the following procedure to view the Ethernet statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, Interface**.
2	Click **Ethernet.** The Ethernet Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Ethernet Statistics page.

Variable	Value
Port	The port number with lowest path cost from the bridge to the common internal spanning tree (CIST) root bridge.
Port Name	The port name.

Variable	Value
Alignment Errors	The number of received frames, which are not an integral number of octets in length and fail frame check sequence (FCS) check.
FCS Errors	The number of received frames, which are integral number of octets in length and fail FCS check.
Single Collision Frames	The number of transmitted frames, with a single collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
SQE Test Errors	The number of times the SQE TEST ERROR message the PLS sublayer generates for a particular interface. Configure the SQE TEST ERROR in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in Institute of Electrical and Electronics (IEEE) Std. 802.3, 1998 Edition, section 7.2.4.6.
Deferred Transmissions	The number of frames, with a delayed first transmission, because of the busy interface. The count represented by an instance of this object does not include frames involved in collisions.
Late Collisions	The number of collisions on an interface after transmission of a packet.
Excess Collisions	The number of frames with failed transmission because of excessive collisions.
Transmitted Internal MAC Errors	The number of frames with failed transmission because of internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times the carrier sense loses during transmission of a frame.
Frame Too Long	The number of received frames with a size more than maximum permitted frame size.
Received Internal MAC Errors	The number of received frames, with failed transmission, because of internal MAC sublayer transmit error.
Ether Chipset	The object that identifies the chipset to realize the interface.
Symbol Errors	For an interface with a speed of 100 mega bits per second, the number of times with invalid data symbol when a valid carrier exists.
Duplex Status	The current mode of the port entity.

Viewing wireless statistics

Use the following procedure to view the wireless local area network (WLAN) statistics of BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, Wireless**. The WLAN Station Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the WLAN Station Statistics page.

Variable	Value
Station Address	The MAC address that identifies the stations in the AP.
SSID	The SSID that authorizes the station.
Vlan ID	The VLAN tag on the packets from the station. The range of the ID is any number except 4093.
Authentication status	The status of the authentication.
Association status	The associating status of the station.
Authorization status	The authorization status of the WLAN.
Association ID	The association ID of the station.
Authentication Type	The type of authentication. Options: open shared wpa wpa2 wpawpa2mixed wpapsk wpa2psk wpawpa2pskmixed open1x
Encryption Type	The type of encryption the station uses. Options: staticwep dynamicwep nokey aes tkip aestkip aeswep tkipwep aestkipwep
Transmitted Bytes	The number of bytes per station transmits.
Received Bytes	The number of bytes per station receives.
Transmitted Packets	The number of packets per station transmits.
Received Packets	The number of packets per station receives.

VLAN Statistics

There are two types of statistics that measure Virtual Local Area Network (VLAN) performance. They are VLAN filtering database (FDB) entries and multicast table statistics.

Navigation

- Viewing VLAN FDB Entries (page 73)
- Viewing VLAN Multicast Table (page 73)

Viewing VLAN FDB Entries

Use the following procedure to view the VLAN FDB entries statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VLAN**. The VLAN FDB Entries dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VLAN FDB Entries page.

Variable	Value
VLAN ID	The VLAN ID for which you get filtering database information.
MAC Address	The MAC address for which the VLAN mapping exists in the entry.
Port	The port type.
All	All filtering database information in the BSG.
Status	The configuring status of the FDB entry. The status can be manual or static. Options: deleteOnReset deleteOnTimeout

Viewing VLAN Multicast Table

Use the following procedure to view the VLAN FDB entries statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VLAN**.
2	Click **Multicast Table.** The VLAN Multicast Table dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VLAN Multicast Table page.

Variable	Value
VLAN ID	The VLAN ID for which you obtain the filtering database information.
Address	The address for which the VLAN mapping exists in the entry.
Egress Ports	The set of ports which receive frames from a specific port. From these ports frames are forwarded to a specific multicast or broadcast MAC address.
Ports Learnt	The interfaces of the multicast entry.

MSTP Statistics

Use the following procedures to measure Multi-Service Transport Protocol (MSTP) performance.

Navigation

- Viewing MSTP information (page 74)
- Viewing CIST port statistics (page 75)
- Viewing MSTI port statistics (page 76)

Viewing MSTP information

Use the following procedure to view the MSTP information for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, MSTP**. The MSTP Information dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the MSTP Information page.

Variable	Value
Address	The unique MAC address used by the BSG.
Cist Root	The bridge identifier of the common spanning tree (CST) root.
Regional Root	The unique bridge identifier of the bridge recorded as the CIST Regional Root Identifier in the configuration BPDUs transmitted.
Cost Root Port	The associated cost of the path to the CIST root as seen from the bridge.
Hold Time (Seconds)	The time period, in seconds, which determines the interval length that is not more than two configuration bridge PDUs the node transmits.
Max Age (Seconds)	The maximum age of the STP information that is learnt from the network on any port before it is discarded. The value, in seconds, is the current value of the bridge.
Forward Delay (Seconds)	The time period in seconds, that controls the speed of the spanning tree status changes when it moves to the next state. The value determines how long the port stays in a particular state before moving to the next state.
Configuration Digest	The configuration digest value for the region.
Regional Configuration Digest	The configuration digest value for the region.
Change Count	The number of times a region configuration identifier changes. This event generates a trap.
Time since Topology Change	The time period in seconds that the TcWhile timer in this bridge is zero for CST.
Topology Changes	The number of times when the TcWhile timer is not zero.
New Root Bridge Count	The number of times the root bridge changes. This event generates a trap.

Viewing CIST port statistics

Use the following procedure to view the MSTP CIST port statistics for BSG.

Procedure steps

1. From the BSG navigation panel, select **Device Monitoring, Statistics, MSTP**.
2. Click **CIST Port Statistics.**

   The MSTP CIST Port Statistics dialog box appears.
3. Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the MSTP CIST Port Statistics page.

Variable	Value
Port	A port number with lowest path cost from the bridge to the CIST Root bridge.
Port Name	The name of the interface. The name is assigned by the BSG.
Received MSTP BPDUs	The number of MST BPDUs received on a specific port.
Received RST BPDUs	The number of RST BPDUs received on this port.
Received Config BPDUs	The number of configuration BPDUs received on the specific port.
Received TCN BPDUs	The number of TCN BPDUs received on the specific port.
Transmitted MST BPDUs	The number of MST BPDUs that the port transmits.
Transmitted RST BPDUs	The number of RST BPDUs that the port transmits.
Transmitted Config BPDUs	The number of configuration MST BPDUs that the port transmits.
Transmitted TCN BPDUs	The number of TCN BPDUs that the port transmits.
Received Invalid MST BPDUs	The number of invalid MST BPUDs received on the port.
Received Invalid RST BPDUs	The number of invalid MST BPUDs received on the port.
Received Invalid Config BPDUs	The number of invalid configuration BPDUs received on the port.
Protocol Migration Count	The number of times the port is migrated from one STP version to another STP version.

Viewing MSTI port statistics

Use the following procedure to view the multi-service transport instance port statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, MSTP**.
2	Click **MSTI Port Statistics.** The MSTP MSTI Port Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the MSTP MSTI Port Statistics page.

Variable	Value
Instance	The spanning tree instance.
Port Name	The name of the interface. The name is assigned by the BSG.
Received MSTP BPDUs	The number of MST BPDUs received on a specific port.
Received Config BPDUs	The number of configuration BPDUs received on the specific port.
Received TCN BPDUs	The number of TCN BPDUs received on the specific port.
Transmitted MST BPDUs	The number of MST BPDUs that the port transmits.
Transmitted RST BPDUs	The number of RST BPDUs that the port transmits.
Transmitted Config BPDUs	The number of configuration MST BPDUs that the port transmits.
Transmitted TCN BPDUs	The number of TCN BPDUs that the port transmits.
Received Invalid MST BPDUs	The number of invalid MST BPUDs the port receives.
Received Invalid RST BPDUs	The number of invalid MST BPUDs the port receives.
Received Invalid Config BPDUs	The number of invalid configuration BPDUs the port receives.
Protocol Migration Count	The number of times the port migrates from one STP version to another STP version.

RSTP Statistics

There are two types of statistics that measure Rapid Spanning Tree Protocol (RSTP) performance. They are RSTP information and RSTP port statistics.

Navigation

- Viewing RSTP information (page 77)
- Viewing RSTP port statistics (page 78)

Viewing RSTP information

Use the following procedure to view the RSTP information for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, RSTP**. The RSTP Information dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the RSTP Information page.

Variable	Value
Address	The unique MAC address used by the BSG.
Protocol Specification	The version of the running STP. Options: decLb100 ieee8021d.
Time since Topology Change	The time period in seconds from the TcWhile timer in this bridge is zero for CST.
Topology Changes	The number of times when the TcWhile timer is non-zero.
Designated Root	The bridge identifier of the root of the spanning tree.
Root Cost	The cost of the associated path to the root as seen from the bridge.
Root Port	The port number which offers lowest cost for the path from the bridge to the root bridge.
Max Age (Seconds)	The maximum age of the STP information that the network learns on any port before the port discards. The value is in seconds and is the current value of the bridge.
Hello Time (Seconds)	The time period in seconds, between the transmission of configuration bridge PDUs by this node on any port. This is the current bridge value.
Hold Time (Seconds)	The time period in seconds, which determines the interval length which is not more than two configuration bridge PDUs will be transmitted by this node.
Forward Delay (Seconds)	The time period in seconds, that controls the speed of the spanning tree status changes when it moves to the next state. The value determines how long the port stays in a particular state before moving to the next state.

Viewing RSTP port statistics

Use the following procedure to view the RSTP port statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, RSTP**.
2	Click **Port Statistics.** The RSTP Port Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the RSTP Port Statistics page.

Variable	Value
Port	The unique port number.
Port Name	The name of the interface. The BSG assigns the name.
Received RSTP BPDUs	The number of RST BPDUs the port receives.
Received Config BPDUs	The number of configuration BPDUs the port receives.
Received TCN	The number of TCN BPDUs the port receives.
Transmitted RST BPDUs	The number of RST BPDUs the port transmits.
Transmitted Config BPDUs	The number of MST BPDUs the port transmits.
Transmitted TCN	The number of TCN BPDUs the port transmits.
Received Invalid RST BPDUs	The number of invalid MST BPUDs the port receives.
Received Invalid TCN BPDUs	The number of invalid configuration BPDU the port receives. This event generates a trap.
Protocol Migration Count	The number of times the port migrates from one STP version to another. This event generates a trap.

802.1x statistics

There are five types of statistics that measure 802.1x performance: port based, MAC based, authenticator statistics, supplicant statistics, and MAC session statistics.

Navigation

- Viewing 802.1x port based session statistics (page 79)
- Viewing 802.1x MAC based statistics (page 80)
- Viewing 802.1x authenticator statistics (page 81)
- Viewing 802.1x supplicant statistics (page 82)
- Viewing 802.1x MAC session statistics (page 83)

Viewing 802.1x port based session statistics

Use the following procedure to view the 802.1x port based session statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, 802.1x**. The 802.1x Port Based Session Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the 802.1x Port Based Session Statistics page.

Variable	Value
Port	The port number. The value must be greater than zero.
Port Name	The name of the interface. The BSG assigns the name.
Session ID	The session identifier of the supplicant.
Received Frames	The number of session frames the supplicant receives.
Transmitted Frames	The number of session frames the supplicant transmits.
Session Time (Seconds)	The time period of the session in seconds.
Session Terminate Cause	The reason that terminates the session.
User Name	The user name that identifies the supplicant PAE.

Viewing 802.1x MAC based statistics

Use the following procedure to view the 802.1x media access control (MAC) based statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, 802.1x**.
2	Click **MAC Based.** The 802.1x MAC Based Session Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the 802.1x MAC Based Session Statistics page.

Variable	Value
MAC Address	The MAC address of the supplicant.
Octet Received	The number of session octets the supplicant receives.
Octets Transmitted	The number of session octets the supplicant transmits.
Frames Received	The number of session frames the supplicant receives.
Frames Transmitted	The number of session frames the supplicant receives.

Variable	Value
Session ID	The unique session identifier of the session.
Authentication Method	The authentication method in use to establish the session. Options: remoteAuthServer localAuthServer
Session Time (Seconds)	The time period of the session in seconds.
Session Terminate Cause	The reason that terminates the session.
User Name	The user name that identifies the supplicant PAE.

Viewing 802.1x authenticator statistics

Use the following procedure to view the 802.1x authenticator statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, 802.1x**.
2	Click **Authenticator.** The Authenticator Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Authenticator Statistics page.

Variable	Value
Port	The port number.
Port Name	The name of the interface. The BSG assigns the name.
EAPOL Frames Received	The number of valid Extensible Authentication Protocol Over LANs (EAPOL) received by the authenticator.
Frames Transmitted	The number of session frames the authenticator transmits.
Start Frames	The number of EAPOL start frames the authenticator receives.
Logoff Frames Received	The number of EAPOL logoff frames the authenticator receives.
Resp/ID Frames Received	The number of Extensible Authentication Protocol (EAP) response ID frames the authenticator receives.
Response Frames Received	The number of valid EAP response frames the authenticator receives.
Req/ID Frames Transmitted	The number of EAP required ID frames the authenticator receives.
Request Frames Transmitted	The number of EAP request frames the authenticator receives.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames the authenticator receives.

Variable	Value
Error Frames Received	The number of EAPOL frames with invalid packet body field lengths the authenticator receives.
EAPOL Frame Versions	The protocol version number of the current EAPOL frame.
EAPOL Frame Source	The source MAC address of the current EAPOL frame.

Viewing 802.1x supplicant statistics

Use the following procedure to view the 802.1x supplicant statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, 802.1x**.
2	Click **Supplicant.** The Supplicant Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Supplicant Statistics page.

Variable	Value
Port	The port number.
Port Name	The name of the interface. The BSG assigns the name.
Start Frames	The number of EAPOL start frames the supplicant transmits.
Resp/ID Frames Transmitted	The number of EAP response ID frames the supplicant transmits.
Response Frames Transmitted	The number of valid EAP response frames the supplicant transmits
Logoff Frames Transmitted	The number of EAPOL logoff frames the supplicant transmits
Total Frames Transmitted	The number of all EAPOL frames the supplicant transmits.
Req/ID Frames Received	The number of EAP required ID frames the supplicant receives.
Request Frames Received	The number of EAP request frames the supplicant receives. The number excludes request ID frames.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames the supplicant receives.
Error Frames Received	The number of EAPOL frames with invalid packet body field lengths the supplicant receives.
Total frames Received	The number of all EAPOL frames the supplicant receives.
EAPOL Frame Versions	The protocol version number of the current EAPOL frame.
EAPOL Frame Source	The source MAC address of the current EAPOL frame.

Viewing 802.1x MAC session statistics

Use the following procedure to view the 802.1x supplicant statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, 802.1x**.
2	Click **MAC Session Statistics.** The MAC Session Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the MAC Session Statistics page.

Variable	Value
Supplicant MAC Address	The port number.
Frames Received	The number of session frames the supplicant receives.
Frames Transmitted	The number of session frames the supplicant transmits.
Session Id	The unique session identifier.
Session Terminate Cause	The reason that terminates the session.
User Name	The user name that identifies the supplicant PAE.

IP Statistics

There are four types of statistics that measure Internet Protocol (IP) performance. They are IP interfaces, Address Resolution Protocol (ARP) cache, IP statistics, and Internet Control Message Protocol (ICMP) statistics.

Navigation

- Viewing IP interfaces (page 83)
- Viewing ARP Cache (page 85)
- Viewing IP Statistics (page 85)
- Viewing ICMP Statistics (page 86)

Viewing IP interfaces

Use the following procedure to view IP interfaces configured on the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IP**. The IP Interfaces dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the IP Interfaces page.

Variable	Value
IP Interface	The identifying value of the interface.
IP Address	The IP address related to the client hardware address.
Subnet Mask	The network to which the IP address belongs.
Broadcast Address	The broadcast address.
IP Assignment	The IP assignment mode of the interface. Options: Dynamic—external agent assigns the IP address. Static—user assigns the IP address.
Network type	The network type. Options: Local Area Network (LAN) Wide Area Network (WAN)
Link type	The network access type. Options: Private—LAN. Public—WAN.
Nat Status	The NAT status. Options: Enabled—WAN interface. Disabled—LAN interface.
Firewall Status	The firewall status. Options: Enabled—default for WAN interface. Disabled—default for LAN interface.
Interface Status	The current status of the interface. Options: UP DOWN

Viewing ARP Cache

Use the following procedure to view ARP cache of the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IP**.
2	Click **ARP Cache.** The ARP Cache dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the ARP Cache page.

Variable	Value
Interface	The interface that receives the ARP.
MAC Address	The MAC address that sends the ARP packet.
IP Address	The IP address that sends the ARP packet.
Media Type	The ARP entry type. Options: Dynamic—learn dynamically. Static—configure statically.

Viewing IP Statistics

Use the following procedure to view IP statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IP**.
2	Click **IP Statistics.** The IP Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the IP Statistics page.

Variable	Value
Total Received Messages	The total number of messages the interface receives.
Header Error Discards	The number of input datagrams the interface discards because of errors in the IP headers. The errors also include bad checksums, version number mismatch, other format errors, time-to-live exceeded, and errors discovered in IP processing.
Bad IP Discards	The total number of input datagrams the interface discards with invalid IP addresses.
Unsupported Protocol Discards	The number of local datagrams the interface receives successfully, but discards because of unknown or unsupported protocols.
Reassembled Packets	The number of successful re-assembled IP datagrams.
Reassembly Timeouts	The maximum period of time, in seconds, during which the received fragments await reassembly at this entity.
Reassembly Required	The number of IP fragments the interface receives that need reassembling at this entity.
Fragmented Packets	The number of fragmented IP datagrams at this entity.
Broadcast Packets Forwarded	The number of input datagrams for which this entity is not the final IP destination of the packet. As a result, the system finds route to use to forward the packets to the final destination.
Generated Broadcast Requests	The total number of supplied IP datagrams that the interface transmits on request.
Dropped Packets	The number of IP datagrams that the interface discards because of unavailable routes.

Viewing ICMP Statistics

Use the following procedure to view Internet Control Message Protocol (ICMP) statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IP**.
2	Click **ICMP Statistics.**
	The ICMP STatistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the ICMP Statistics page.

Variable	Value
Received Message	The number of ICMP messages the entity receives, including the error packet.
Received Error	The number of ICMP messages with errors, such as bad ICMP checksums or bad length.
Receive Destination Unreachable	The number of unreachable ICMP destination messages the entity receives.
Received Redirect	The number of ICMP redirects the entity receives.
Received Echo Requests	The number of ICMP echo requests the entity receives.
Received Echo Replies	The number of ICMP echo replies the entity receives.
Receive Source Quenches	The number of ICMP source quench messages the entity receives.
Transmitted Message	The number of ICMP messages the entity sends. The number includes the error packets.
Transmitted Error	The number of unsent ICMP messages with errors.

Viewing DHCP Statistics

Use the following procedure to view the Dynamic Host Configuration Protocol (DHCP) server binding table of the BSG.

Navigation

- “Viewing DHCP binding statistics” on page 87
- “Viewing DHCP server statistics” on page 88

Viewing DHCP binding statistics

Use this procedure to view DHCP binding statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, DHCP, Binding**. The DHCP Binding Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the DHCP Server Binding Statistics page.

Variable	Value
IP Address	The IP address associated with the binding.
Hardware Address	The hardware address of the binding. The value is zero for the client identifier.
Expiry Time(secs)	The remaining time for the binding in seconds. Expired bindings have negative value.
Binding State	The binding state. Options: Offered—the server sends the offer and waits for a client request. Assigned—the server assigns the address to the client. Probing—the DHCP server probes the address.

Viewing DHCP server statistics

Use this procedure to view DHCP server statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, DHCP, Server**. The DHCP Server Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the DHCP Server Statistics page.

Variable	Value
Total Address Pools	The number of configured DHCP pools configured in the system.
Total DHCP Offer Sent	The number of DHCP Offer packets the server sends.
Total DHCP Ack Sent	The number of DHCP ACK packets the server sends.
Total DHCP Nack Sent	The number of DHCP NACK packets the server sends.
Total DHCP Discover Received	The number of DHCP Discover packets the server receives.
Total DHCP Request Received	The number of DHCP Request packets the server receives.
Total DHCP Decline Received	The number of DHCP Decline packets the server receives.

Variable	Value
Total DHCP Release Received	The number of DHCP Release packets the server receives.
Total DHCP Informs Received	The number of DHCP Informs packets the server receives.

Viewing DHCP relay statistics

Use this procedure to view DHCP relay statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, DHCP Relay**. The DHCP Relay Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the DHCP Relay Statistics page.

Variable	Value
Dhcp Relay	The status of the relay agent. If you enable this variable, the relay agent activates.
Dhcp Relay Servers Only	If you enable this variable, the relay agent forwards the packets from the client to a specific DHCP server.
Dhcp Relay RAI Option	If you enable this variable, the relay agent handles the processing related to Relay Agent Information (RAI) options.
Debug Level	The trace level object with the bit masks for various levels of tracing.
Packets Inserted RAI Option	The number of packets the relay agent inserts with the RAI option.
Packets Inserted Circuit ID Suboption	The number of packets the relay agent inserts with the Circuit ID suboption.
Packets Inserted Remote ID Suboption	The number of packets the relay agent inserts with the Remote ID suboption.
Packets Inserted Subnet Mask Suboption	The number of packets the relay agent inserts with the Subnet Mask suboption.
Packets Dropped	The number of packets the relay agent drops.
Packets Not Inserted RAI Option	The number of packets in which the RAI Option was not inserted by the Relay Agent. If inserted, the packet size will exceed the MTU.

Viewing RIP Statistics

Use the following procedure to view the Routing Information Protocol (RIP) statistics of BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, RIP**. The RIP Interface Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the RIP Interface Statistics page.

Variable	Value
IP Address	The IP address of the interface on which you configure the RIP.
Received Bad Packets	The number of RIP packets the interface discards.
Received Bad Routes	The number of rejected routes.
Transmitted Updates	The number of triggered RIP updates the interface sends. The number does not include all new information.
Periodic Updates	The number of triggered RIP updates the interface sends. The number includes all new information.
Admin Status	The RIP status.

OSPF Statistics

There are two types of statistics that measure Open Shortest Path First (OSPF) protocol performance. They are OSPF and OSPF interface statistics.

Navigation

- Viewing OSPF statistics (page 90)
- Viewing OSPF Interface statistics (page 91)

Viewing OSPF statistics

Use the following procedure to view the total number of OSPF packets received, transmitted, or discarded by the BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, OSPF**. The OSPF Statistics dialog box appears.

2 Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the OSPF Statistics page.

Variable	Value
OSPF Packets Received	The number of OSPF packets the interface receives.
OSPF Packets Transmitted	The number of OSPF packets the interface transmits.
OSPF Packets Discards	The number of OSPF packets the interface discards.

Viewing OSPF Interface statistics

Use the following procedure to view the OSPF statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, OSPF**.
2	Click **Interface.** The OSPF Interface Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the OSPF Interface Statistics page.

Variable	Value
Interface	The IP address of the interface on which you configure the OSPF.
Discarded Hello	The number of Hello packets the interface discards.
Received Hello	The number of Hello packets the interface receives.
Received LSA Acknowledgements	The number of link state advertisement (LSA) acknowledgements on this interface.
Received LSA Requests	The number of LSA requests the interface receives.
Received LSU	The number of link state update (LSU) packets the interface receives.
Transmitted Database Description	The number of database description packets the interface transmits.
Transmitted Hello	The number of hello packets the interface transmits.
Transmitted LSA Acknowledgements	The number of LSA acknowledgements the interface transmits.

Variable	Value
Transmitted LSA Requests	The number of LSA requests the interface transmits.
Transmitted LSU	The number of LSA packets the interface transmits.

Viewing VRRP Statistics

Use the following procedure to view the Virtual Router Redundancy Protocol (VRRP) statistics of BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VRRP**. The VRRP Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VRRP Statistics page.

Variable	Value
Version Errors	The number of VRRP packets the router receives with invalid VRRP checksum values.
Virtual Router ID Errors	The number of VRRP packets the router receives with unknown or unsupported version numbers.
Virtual Router ID	The virtual ID associated with the virtual router.
Transitions to Master	The number of times the virtual router state transitions to Master.
Advertisement Receive	The number of VRRP advertisements the virtual router receives.
Advertisement Internal Error	The number of VRRP advertisement packets the router receives with advertisements interval different from the one configured for the local virtual router.
Authentication Failures	The number of VRRP packets the router receives with failed authentication checks.
IP TTL Errors	The number of VRRP packets the router receives with IP Time-To-Live (TTL) not equal to 255.
Priority Zero Packet Received	The number of VRRP packets the virtual router receives with a priority of zero.
Priority Zero Packet Transmitted	The number of VRRP packets the virtual router sends with a priority of zero.
Invalid Packet Type Received	The number of VRRP packets the router receives with an invalid type.
Address List Errors	The number of packets the router receives for which the address list does not match the locally configured list for the virtual router.

Variable	Value
Invalid Authentication Type	The number of packets with an unknown authentication type.
Authentication Type Mismatch	The number of packets with an authentication type that does not match the locally configured authentication.
Packet Length Errors	The number of packets with a length less than VRRP header length.

IGMP Snooping Statistics

There are two types of statistics that measure Internet Group Management Protocol (IGMP) snooping performance. They are IGS V1/V2 and IGS V3 statistics.

Navigation

- Viewing IGS V1/V2 statistics (page 93)
- Viewing IGS V3 statistics (page 94)

Viewing IGS V1/V2 statistics

Use the following procedure to view the Internet Go Server (IGS) V1/V2 statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IGMP Snooping**. The IGS V1/V2 Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the IGS V1/V2 Statistics page.

Variable	Value
VLAN ID	The VLAN ID for IGMP snooping configuration.
General Queries Received	The statistics for the general queries the snooping switch receives.
Group Queries Received	The statistics for the group specific queries the snooping switch receives.
Group and Source Queries Received	The statistics for group and source specific queries received by the snooping switch.
IGMP Reports Received	The IGMP V3 membership report statistics the snooping switch receives.

Variable	Value
IGMP Leaves Received	The statistics for the IGMP V2 leave messages the snooping switch receives.
IGMP Packets Dropped	The number of erroneous IGMP packets the snooping switch rejects due to checksum calculation failure.
General Queries Transmitted	The general queries statistics the snooping switch transmits.
Group Queries Transmitted	The statistics for the group specific queries the snooping switch transmits.
IGMP Reports Transmitted	The statistics for the IGMP V1 and IGMP V2 membership reports the snooping switch transmits.
IGMP Leaves Transmitted	The statistics for the IGMP V2 leave messages the snooping switch transmits.

Viewing IGS V3 statistics

Use the following procedure to view the IGS V3 statistics for BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, IGMP Snooping**.
2	Click **IGS V3 Statistics.** The IGS V3 Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on IGS V3 Statistics page.

Variable	Value
VLAN ID	The VLAN ID in which the IGS receives the packets.
V3 Reports Received	The statistics of the IGMP V3 membership reports the snooping switch receives.
IS_INCL Messages Received	The statistics of the IS_IN IGMP V3 reports the snooping switch receives with a message type of IS_IN.
IS_EXCL Messages Received	The statistics of the IS_EX IGMP V3 membership the snooping switch receives with a message type of IS_EX.
TO_INCL Messages Received	The statistics for the IGMP V3 membership the snooping switch receives with a message type of TO_IN.
TO_EXCL Messages Received	The statistics of the IGMPv3 membership reports of type IS_IN received by the snooping switch.

Variable	Value
ALLOW Messages Received	The statistics of the IGMPV3 membership the snooping switch receives with a message type of ALLOW.
BLOCK Messages Received	The statistics of the IGMPV3 membership the snooping switch receives with a message type of BLOCK.
V3 Reports Sent	The statistics of the IGMPV3 the snooping switch transmits.

Configuring and viewing RMOM statistics

This section provides procedures for configuring and viewing RMON performance information.

Navigation

- Configuring RMON Ethernet statistics (page 95)
- Configuring RMON history (page 96)
- Viewing RMON Statistics (page 97)

Configuring RMON Ethernet statistics

Use the following procedure to configure Ethernet statistics for RMON.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, RMON.**
2	Click **Ethernet Statistics.**
	The Ethernet Statistics Configuration dialog box appears.
3	In the **Index** field, type the index number.
4	In the **Port Name** list, select the port name.
5	In the **Owner** field, type the name of the owner.
6	Click **Add.**

End

Variable definitions

Use the data in the following table to configure ethernet statistics for RMON.

Variable	Value
Index	Specifies the ethernet statistics index that uniquely identifies an entry in the Ethernet Statistics table.

Variable	Value
Port Name	Specifies the port name for the entry.
Owner	Specifies the owner name.

Configuring RMON history

Use the following procedure to configure how RMON statistics are collected.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, RMON.**
2	Click **History.**
	The History Control Configuration dialog box appears.
3	In the **Index** field, type the index number.
4	In the **Port Name** list, select the port name.
5	In the **Buckets Requested** field, type the number of buckets requested.
6	In the **Interval** field, type the time interval between two successive pollings.
7	In the **Owner** field, type the name of the owner.
8	Click **Add.**

End

Variable definitions

Use the data in the following table to configure history control for RMON.

Variable	Value
Index	Specifies the index that uniquely identifies an entry in the history control table.
Port Name	Specifies the port name for which the history information is configured.
Buckets Requested	Specifies the number of buckets to be configured to collect the RMON statistics; that is, the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with that entry. The configuring values range from 1 to 65535. The default value is 50.
Buckets Granted	Specifies the number of buckets granted to collect the RMON statistics. The configuring values range from 1 to 65535.

Variable	Value
Interval	Specifies the time interval between two successive polling to collect the statistics. The configuring values range from 1 and 3600. The default value is 1800.
Owner	Specifies the owner name.

Viewing RMON Statistics

Use the following procedure to view the Remote Monitoring (RMON) Ethernet statistics of BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, RMON**. The RMON Ethernet Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the RMON Ethernet Statistics page.

Variable	Value
Index	The unique identity of the etherStats entry.
Data Source	The identity of data source for which you configure the entry. This source can be any ethernet interface on the device.
Drop Events	The number of events in which the RMON rejects the packets due to lack of resources.
Packets	The number of bad packets, broadcast packets, and multicast packets the RMON receives.
Broadcom Packets	The number of good packets, excluding multicast packets, the RMON receives that are directed to a broadcast address.
Multicast Packets	The number of good packets which RMON directs to a multicast address. This number excludes the broadcom packets.
CRC Errors	The total number of packets the RMON receives with a length more than 64 octets and less than 1518 octets. This number includes the FCS octets and excludes framing bits. The packets can include one of the following errors: FCS Error—bad FCS with an integral number of octets. Alignment Error—bad FCS with a nonintegral number of octets
Under Size Packets	The number of packets the RMON receives with a length less than 64 octets.

Variable	Value
Over Size Packets	The number of packets the RMON receives with a length longer than1518 octets. This number excludes framing size and includes FCS octets.
Fragments	The total number of packets the RMON receives with a length less than 64 octets. This number includes the FCS octets and excludes framing bits. The packets can include one of the following errors: FCS Error—bad FCS with an integral number of octets. Alignment Error—bad FCS with a non-integral number of octets.
Jabbers	The total number of packets the RMON receives with a length longer than 1518 octets. This number includes the FCS octets and excludes framing bits. The packets can include one of the following errors: FCS Error—bad FCS with an integral number of octets. Alignment Error—bad FCS with a nonintegral number of octets.
Collisions	The number of collisions on the Ethernet segment. The value depends on the location of the RMON probe.
64 Octets	The number of good and bad packets with a length of 64 octets. This number excludes the framing bits but includes the FCS octets.
65.127 Octets	The number of good and bad packets with a length more than 65 octets and less than 127 octets. This number includes the FCS octets and excludes framing bits.
128.255 Octets	The number of good and bad packets with a length more than 128 octets and less than 255 octets. This number includes the FCS octets and excludes framing bits.
256.511 Octets	The number of good and bad packets with a length more than 256 octets and less than 511 octets. This number includes the FCS octets and excludes framing bits.
512.1023 Octets	The number of good and bad packets with a length more than 512 octets and less than 1023 octets. This number includes the FCS octets and excludes framing bits.
1024.1518 Octets	The number of good and bad packets with a length more than 1024 octets and less than 1518 octets. This number includes the FCS octets and excludes framing bits.

Viewing NAT statistics

On the NAT pages, you can view Network Address Translation (NAT) statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, NAT**. NAT Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the NAT Statistics page.

Variable	Value
Interface Name	The global interface number on which the session runs.
Local IP Address	The IP address of the host connected to the network.
Translated IP	The IP address of the local host assigned by NAT. The external host communicates to the local host with this address.
Local Port	The source or destination port that the local host uses to communicate with the external network.
Translated Port	The port number assigned by the NAT when you enable Process Analytical Technology (PAT); otherwise the original port number is used.
Global IP Address	The IP address of the external host with which the local host communicates.
Outside Port	The communicating port number of the external host.

Viewing firewall statistics

Use the following procedure to view the firewall statistics of BSG.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, FIREWALL**. The Firewall Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Firewall Statistics page.

Variable	Value
Total Packets Inspected	The number of packets the firewall module inspects. The number includes the number of packets rejected and accepted.
Total Packets Dropped	The number of packets the firewall module rejects.
Total Packets Accepted	The number of packets the firewall module accepts.
ICMP Packets Dropped	The number of ICMP packets the firewall module rejects.
SYN Packets Dropped	The number of SYN packets the firewall module rejects.

Variable	Value
IP Spoofed Packets Dropped	The number of packets the firewall module rejects because of IP spoof attacks on the external interface.
Source Route Packets Denied	The number of packets the firewall module rejects because of source routing attacks on the external interface.
Tiny Fragment Packets Dropped	The number of packets the firewall module rejects because of tiny fragment attacks on the external interface.
Large Fragment Packets Dropped	The number of fragmented packets the firewall rejects.
Packets with IP Options Dropped	The number of packets the firewall module rejects with IP options, such as source routing, record routing, timestrap.
Suspicious Attacks Dropped	The number of packets the firewall module rejects due to suspicious attacks, such as LAN attack, SMURF attack, and ICMP Short Header.

Viewing VPN statistics

On the VPN pages, you can view the Virtual Private Network (VPN) statistics.

VPN navigation

- "VPN Statistics" (page 100)
- "VPN IKE Statistics" (page 101)
- "VPN IPSEC Statistics" (page 101)

VPN Statistics

Use the following procedure to view the statistics for the VPN.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VPN, Global Statistics**. The VPN Global Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VPN Statistics page.

Variable	Value
Maximum Tunnels Supported	The number of maximum tunnels supported by the VPN module.
IP Packets Received	The number of incoming packets through the VPN module.
IP Packets Transmitted	The number of outgoing packets through the VPN module.
IP Packets Secured	The number of packets secured by the VPN module.
IP Packets Dropped	The number of packets dropped by the VPN module.

VPN IKE Statistics

Use the following procedure to view the VPN Internet Key Exchange (IKE) statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VPN, IKE Statistics**. The VPN IKE Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VPN IKE Statistics page.

Variable	Value
IKE Active Security Associations	The number of active IKE security associations in the VPN module.
IKE Negotiations	The number of IKE security associations negotiated in the VPN module.
IKE Security Associations Re-Keyed	The number of IKE security associations rekeyed.
IKE Negotiations Failed	The number of failed IKE security association negotiations.

VPN IPSEC Statistics

Use the following procedure to view statistics about the configured VPN IPsec protocol.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, VPN, IPSEC Statistics**. The VPN IPSEC Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the VPN IPSEC Statistics page.

Variable	Value
IPSEC Active Security Associations	The number of active IPSEC security associations in the VPN module.
IPSEC Negotiations	The number of IPSEC security negotiations in the VPN module.
IPSEC Negotiations Failed	The number of failed IPSEC security negotiations negotiations.
IPSEC Security Associations Re-Keyed	The number of IPSEC security associations rekeyed.

Viewing DSL Line statistics

Use the following procedure to view DSL Line statistics on the BSG12aw.

Procedure steps

Step	Action
1	From the navigation panel, select **Device Monitoring, Statistics, DSL Line**. The DSL Line Statistics dialog box appears.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the DSL Line Statistics page.

Variable	Value
DSL Line	The DSL Line type.
Firmware Version	The firmware version.
Operational Status	The operational status of the DSL modem.
Received AAL5 CRC Errors	The number of AAL5 CRC errors received.

Variable	Value
Received ATM HEC Errors	The number of ATM HEC errors.
Received Packets	The number of packets coming into the modem from the WAN interface.
Received Octets	The number of octets coming into the modem from the WAN interface.
Received Cells	The number of cells coming into the modem from the WAN interface.
Transmitted Octets	The number of octets transmitted from the modem to the WAN interface.
Transmitted Cells	The number of cells transmitted from the modem to the WAN interface.

Viewing T1/E1 statistics

There are three types of statistics that measure T1/E1 performance: current statistics, interval statistics, and total statistics.

Navigation

- Viewing T1/E1 current statistics (page 103)
- Viewing T1/E1 interval statistics (page 104)
- Viewing T1/E1 total statistics (page 106)

Viewing T1/E1 current statistics

Use the following procedure to view T1/E1 current statistics on the BSG12tw.

Procedure steps

Step	Action
1	From the navigation panel, select **Device Monitoring, Statistics, T1/E1**. The T1/E1 Current Statistics dialog box appears.
2	Select the T1/E1 interface to view.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the T1/E1 Current Statistics page.

Variable	Value
Interface	The T1/E1 controller.
Errored Seconds	The number of errored seconds (ES). An ES has: • one or more path coding violations • one or more out of frame (OOF) defects • one or more controlled slip events • a detected alarm indication signal (AIS) defect
Severely Errored Seconds	The number of severely errored seconds.
Severely Errored Framing Seconds	The number of seconds with one or more OOF defects or an AIS defect.
Unavailable Seconds	The number of unavailable seconds.
Controlled Slip Seconds	The number of controlled slip seconds. Controlled slips occur when there is a difference between the timing of a synchronous receiving terminal and the received signal. A controlled slip does not cause an OOF defect.
Path Coding Violations	The number of path coding violations. These violations occur when there is: • a frame synchronization bit error in the D4 and E1-no CRC formats • a CRC or frame synchronization bit error in the ESF and E1-CRC formats
Line Errored Seconds	The number of line errored seconds. A line errored second occurs when one or more line code violation events are detected.
Bursty Errored Seconds	The number of bursty errored seconds. These occur when there are: • from 2 to 319 path coding violation events • no severely errored frame defects • no detected incoming AIS defects
Degraded Minutes	The number of 60-second periods in which the cumulative errors exceed 1E-6 but do not exceed 1E-3 for the DS-1 path.
Line Code Violations	The number of times the received data was in violation in terms of line coding. Values range from 1 to 65536.

Viewing T1/E1 interval statistics

Use the following procedure to view T1/E1 interval statistics on the BSG12tw.

Procedure steps

Step	Action
1	From the navigation panel, select **Device Monitoring, Statistics, T1/E1 Interval Statistics.** The T1/E1 Interval Statistics dialog box appears.
2	From the **Interface** list, select the T1/E1 interface to view.
3	From the **Interval** list, select the interval number to view.

4 Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the T1/E1 Interval Statistics page.

Variable	Value
Interface	The T1/E1 controller.
Interval Index	The interval number to view. The UI displays data for five consecutive intervals, starting from the interval you select. The maximum number of intervals is 96, and each interval is 15 minutes long.
Errored Seconds	The number of errored seconds (ES). An ES has: • one or more path coding violations • one or more out of frame (OOF) defects • one or more controlled slip events • a detected alarm indication signal (AIS) defect
Severely Errored Seconds	The number of severely errored seconds.
Severely Errored Framing Seconds	The number of seconds with one or more OOF defects or an AIS defect.
Unavailable Seconds	The number of unavailable seconds.
Controlled Slip Seconds	The number of controlled slip seconds. Controlled slips occur when there is a difference between the timing of a synchronous receiving terminal and the received signal. A controlled slip does not cause an OOF defect.
Path Coding Violations	The number of path coding violations. These violations occur when there is: • a frame synchronization bit error in the D4 and E1-no CRC formats • a CRC or frame synchronization bit error in the ESF and E1-CRC formats
Line Errored Seconds	The number of line errored seconds. A line errored second occurs when one or more line code violation events are detected.
Bursty Errored Seconds	The number of bursty errored seconds. These occur when there are: • from 2 to 319 path coding violation events • no severely errored frame defects • no detected incoming AIS defects
Degraded Minutes	The number of 60-second periods in which the cumulative errors exceed 1E-6 but do not exceed 1E-3 for the DS-1 path.
Line Code Violations	The number of times the received data was in violation in terms of line coding. Values range from 1 to 65536.
Valid Data	The validity of the data in the selected interval. Options are: • 1 - Valid data was received in the interval • 0 - Invalid data

Viewing T1/E1 total statistics

Use the following procedure to view T1/E1 total statistics on the BSG12tw.

Procedure steps

Step	Action
1	From the navigation panel, select **Device Monitoring, Statistics, T1/E1 Total Statistics**. The T1/E1 Total Statistics dialog box appears.
2	Select the T1/E1 interface to view.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the T1/E1 Total Statistics page.

Variable	Value
Interface	The T1/E1 controller.
Errored Seconds	The number of errored seconds (ES). An ES has: • one or more path coding violations • one or more out of frame (OOF) defects • one or more controlled slip events • a detected alarm indication signal (AIS) defect
Severely Errored Seconds	The number of severely errored seconds.
Severely Errored Framing Seconds	The number of seconds with one or more OOF defects or an AIS defect.
Unavailable Seconds	The number of unavailable seconds.
Controlled Slip Seconds	The number of controlled slip seconds. Controlled slips occur when there is a difference between the timing of a synchronous receiving terminal and the received signal. A controlled slip does not cause an OOF defect.
Path Coding Violations	The number of path coding violations. These violations occur when there is: • a frame synchronization bit error in the D4 and E1-no CRC formats • a CRC or frame synchronization bit error in the ESF and E1-CRC formats
Line Errored Seconds	The number of line errored seconds. A line errored second occurs when one or more line code violation events are detected.
Bursty Errored Seconds	The number of bursty errored seconds. These occur when there are: • from 2 to 319 path coding violation events • no severely errored frame defects • no detected incoming AIS defects

Variable	Value
Degraded Minutes	The number of 60-second periods in which the cumulative errors exceed 1E-6 but do not exceed 1E-3 for the DS-1 path.
Line Code Violations	The number of times the received data was in violation in terms of line coding. Values range from 1 to 65536.

SIP Statistics

There are three types of statistics that measure SIP performance: summary statistics, method statistics, and response class statistics.

Navigation

- Viewing SIP summary statistics (page 107)
- Viewing SIP methods statistics (page 108)
- Viewing SIP response statistics (page 108)

Viewing SIP summary statistics

Use the following procedure to monitor the performance of the SIP summary on the BSG system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, SIP**. The Summary Statistics dialog box appears.
2	Click **Refresh** to reset the SIP summary statistics.

End

Variable definitions

The following table describes the variables that appear on the Summary Statistics page.

Variable	Value
Requests Received	The number of SIP requests, such as invite, register, ACK, cancel, bye that the SIP server receives.
Responses Received	The number of SIP responses, such as 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx that the SIP server receives.
Total Transactions	The number of SIP transactions that takes place. INVITE-2000K-ACK considers as a one transaction. BYE-2000K considers as another transaction.
Requests Sent	The number of SIP requests the SIP server sends.
Responses Sent	The number of responses the SIP server sends.

Viewing SIP methods statistics

Use the following procedure to monitor the performance of the SIP methods on the BSG system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, SIP**.
2	Click **Methods Statistics.** The Methods Statistics dialog box appears.

End

Variable definitions

The following table describes the variables that appear on the Method Statistics page.

Variable	Value
INVITE received	The number of invite requests the SIP server receives.
ACK received	The number of ACK requests the SIP server receives.
REGISTER received	The number of register requests the SIP server receives.
BYE received	The number of bye requests the SIP server receives.
CANCEL received	The number of cancel requests the SIP server receives.
OPTION received	The number of option requests the SIP server receives.
INFO received	The number of info requests the SIP server receives.
INVITE sent	The number of invite requests the SIP server sends.
ACK sent	The number of ACK requests the SIP server sends.
REGISTER sent	The number of register requests the SIP server sends.
BYE sent	The number of bye requests the SIP server sends.
CANCEL sent	The number of ACK requests the SIP server sends.
OPTION sent	The number of option requests the SIP server sends.
INFO sent	The number of info requests the SIP server sends.

Viewing SIP response statistics

Use the following procedure to monitor the performance of the SIP response on the BSG system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, SIP**.
2	Click **Refresh.** The Response Statistics dialog box appears.

End

Variable definitions

The following table describes the variables that appear on the Response Statistics page.

Variable	Value
1xx received	The number of 1xx informational responses the SIP server receives.
2xx received	The number of 2xx suspense responses the SIP server receives.
3xx received	The number of 3xx redirection responses the SIP server receives.
4xx received	The number of 4xx client error responses the SIP server receives.
5xx received	The number of 5xx server failure responses the SIP server receives.
6xx received	The number of 6xx global failure responses the SIP server receives.
Other Classes received	The future enhancements.
1xx sent	The number of 1xx informational responses the SIP server sends.
2xx sent	The number of 2xx suspense responses the SIP server sends.
3xx sent	The number of 3xx redirection responses the SIP server sends.
4xx sent	The number of 4xx client error responses the SIP server sends.
5xx sent	The number of 5xx server failure responses the SIP server sends.
6xx sent	The number of 6xx global failure responses the SIP server sends.
Other Classes sent	The future enhancements.

Viewing QoS statistics

On QoS pages, you can view statistics about the configured Quality of Service (QoS) in the BSG.

QoS navigation

- "Viewing policer statistics" (page 109)
- "Viewing queue statistics" (page 110)

Viewing policer statistics

Use the following procedure to view the QoS policer statistics.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, QoS, Policer**.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Policer Statistics page.

Variable	Value
Policer ID	The index that counts the policing entries.
In-Profile Packets	The number of in profile packets of a policer that the policer ID identifies.
Out-Profile Packets	The number of out profile packets of a policer that the policer ID identifies.
In-Profile Bytes	The numberof in profile bytes of a policer that the policer ID identifies.
Out-Profile Bytes	The number of out profile bytes of a policer that the policer ID identifies.

Viewing queue statistics

Use the following procedure to view the statistics for a specific queue.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, QoS, Queue**.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Queue Statistics page.

Variable	Value
Port No	The name of the interface.
Queue	The index that counts the queue statistics entries. The value ranges from 0 to 7.
Packets Passed	The number of packets that pass through the specific queue of an interface.
Bytes Passed	The number of bytes that pass through the specific queue of an interface.

Viewing TACACS statistics

Use the following procedure to view statistics on TACACS.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Statistics, TACACS**.
2	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the TACACS Statistics page.

Variable	Value
Authentication	
Starts Sent	Number of authentication start requests you send to the server.
Enables Sent	Number of authentication enable requests you send to the server.
Pass Received	Number of authentication passwords the server receives.
Get User Received	Number of authentication get user requests you receive from the server.
Get Data Received	Number of authentication get data requests you receive from the server.
Follows Received	Number of authentication get follows you receive from the server.
Continues Sent	Number of authentication continue requests you send to the server.
Abort Sent	Number of authentication abort requests you send to the server.
Fail Received	Number of authentication fail notifications you receive from the server.
Get Pass Received	Number of authentication get password notifications you receive from the server.
Errors Received	Number of authentication error notifications you receive from the server.
Restart Received	Number of authentication re start notifications you receive from the server.
Authorization	
Requests Sent	Number of authorization requests you send to the server.
Pass Repl Received	Number of authorization pass replace notifications you receive from the server.
Errors Received	Number of authorization errors you receive from the server.
Session Time-Outs	Number of authorization session timesouts.
Pass Add Received	Number of authorization pass add notifications you receive from the server.
Fails Received	Number of authorization fail notifications you receive from the server.
Follows Received	Number of authorization errors you receive from the server.
Accounting	

Variable	Value
Start Reqs. Sent	Number of accounting start requests sent to the server.
Stop Reqs. Sent	Number of accounting stop requests sent to the server.
Errors Received	Number of accounting errors received from the server.
Session Time-Outs	Number of accounting session timeouts.
Success Received	Number of accounting success received from the server.
Follows Received	Number of accounting follows received from the server.
Malformed Packets Received	Number of Malformed packets received from Server.
Socket Failures	Number of socket failures that occurred.
Connection Failures	Number of connection failures that occurred.

BSG system logs

This chapter describes system logs on the BSG.

Navigation

- Configuring logs (page 113)
- Viewing logs (page 115)
- Transferring logs (page 117)

The following figure shows the procedures that you can use to manage logs on the BSG.

Configuring logs

This section describes the how to enable system logging, configure the syslog IP, and enable e-mail notification on the BSG system.

Navigation

- Enabling system logging (page 113)
- Configuring the syslog IP (page 114)
- Configuring e-mail notification (page 115)

Enabling system logging

Perform the following procedure to configure system logging.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Logging.** The System Logging Configuration dialog box appears.
2	From the **System Logging** list, select as enabled or disabled.
3	From the **Console Logging** list, select as enabled or disabled.
4	From the **Flash Logging** list, select as enabled or disabled.
5	From the **Log Level** list, select the required log level.
6	Click **Apply.**

End

Variable definitions

Use the data in following table to configure system logging.

Variable	Value
System Logging	Specifies the system logging status as enabled or disabled. The default value is Enabled.
Console Logging	Specifies the console logging status as enabled or disabled. If you select enabled, the messages (log and e-mail alert messages) sent to the server also appear on the console. If you select disabled, the messages are sent only to the servers but do not appear on the console. The default value is disabled.
Flash Logging	Specifies the flash logging status as enabled or disabled. The default value is enabled and logs generated will be saved to the file system.
Log Level	Specifies the required log level. Select one of the following options: • Emergencies—for logging messages that are equivalent to panic conditions • Alerts—for logging messages that require immediate attention • Critical—for logging critical errors • Errors—for logging error messages • Warnings—for logging warning messages • Notification—for logging messages that require attention and not errors • Informational—for logging informational messages • Debugging—for logging debug messages The default value is Informational.

Configuring the syslog IP

Perform the following procedure to enable Syslog and configure BSG with the IP address of the syslog server.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Logging.**
2	Click **Syslog.** The Syslog IP Configuration dialog box appears.
3	In the **IP Address** field, type the server IP address.
4	Click **Add.**

End

Variable definitions

Use the data in the following table to configure syslog IP for the system.

Variable	Value
IP Address	Specifies the server IP address.

Configuring e-mail notification

Use the following procedure to configure e-mail notification for the system. The IP address of the mail server is set before you configure values for the Receiver Mail ID and the Sender Mail ID.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Logging.**
2	Click **Email Notification.** The Email Notification Configuration dialog box appears.
3	In the **Mail Server IP** field, type the mail server IP address.
4	In the **Recipient Email Address** field, type the e-mail address of the recipient.
5	In the **Sender Email Address** field, type the e-mail address of the sender.
6	Click **Apply.**

End

Variable definitions

Use the data in the following table to configure e-mail notification for the system.

Variable	Value
Mail Server IP	Specifies the mail server IP address used to send e-mail alerts.
Recipient Email Address	Specifies the receiver mail ID. The default ID is admin@domainname.com.
Sender Email Address	Specifies the sender mail id. The default ID is syslog@domianname.com.

Viewing logs

This section provides procedures for viewing the different types of logs available on the BSG.

Navigation

- Viewing system logs (page 116)
- Viewing the VPN log (page 116)
- Viewing the firewall log (page 117)

Viewing system logs

Perform the following procedure to view system logs for the BSG system. A log file is a collection of individual log events generated by the BSG. An administrator can use log files to monitor and analyze system behavior, user sessions, and events. You can transfer BSG log files from the BSG to a specified location, such as your personal computer; see Transferring logs (page 117) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, System Log.** The System Log Information dialog box appears.
2	Click **Refresh t**o view updated logs, or click **Clear** to clear the log information.

End

Viewing the VPN log

Perform the following procedure to view VPN logs for the BSG system. A log file is a collection of individual log events generated by the BSG. An administrator can use log files to monitor and analyze system behavior, user sessions, and events. You manage log files by transferring selected BSG log archives from the BSG to a specified location, such as your personal computer. You can then view individual log events using the BSG Web UI.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, VPN Log.** The VPN Log Information dialog box appears.
2	Select the number of pages to display from the **Show Last Pages** drop-down menu.
3	Click **Refresh.**

End

Viewing the firewall log

You can view traffic reports about packets that are accepted, allowed to transmit, and dropped. Firewall log page also contains source and destination packets information. You can also view reports about the reasons to accept, allow, or drop the packets.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Firewall Log.**
	The Firewall Log Information dialog box appears.
2	Click **Refresh.**

End

Transferring logs

This section provides information about how to transfer a log file from the BSG to another computer.

Transferring a log file

You can transfer selected BSG log archives from the BSG to a specified location, such as a server. The BSG saves log files in a flat text file format. Each log file contains the system log, the VPN log, and the firewall log. Use this procedure to transfer log files from the BSG to another location.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, Log Transfer.**
	The Log Transfer Settings dialog box appears.
2	From the **Backup To** drop-down menu, select the transfer protocol to use.
3	In the **Server IP Address** field, enter the IP address of the destination server.
4	If you selected FTP as the protocol, enter the user name in the **FTP User Name** field.
5	If you selected FTP as the protocol, enter the password in the **FTP Password** field.
6	In the **File Name** field, enter a name to use for the log file.
7	Click **Apply.**

End

Variable definitions

Use the data in the following table to transfer the BSG log to another destination in your network.

Variable	Value
Backup To	Specify the protocol to use for the transfer. The options are FTP and TFTP.
Server IP Address	Specify the IP address of the destination server where the log will be transferred.
FTP User Name	When you select FTP as the transfer protocol, specify the FTP user name.
FTP Password	When you select FTP as the transfer protocol, specify the FTP password.
File Name	Specify the file name for the log. The default file name is cas.log.

BSG backup and restore

This chapter provides information about how to back up and restore the configuration information on the BSG.

Navigation

- Backing up BSG configuration data (page 119)
- Restoring the BSG (page 120)

Backing up BSG configuration data

Before you back up the BSG, ensure that you have saved configuration changes; see Saving configuration files (page 133) for more information.

Backing up configuration files

Use the following procedure to back up BSG for configuration files.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, Configuration File.**
2	Click **Backup**. The Backup Configuration dialog box appears.
3	Choose the type of backup to perform: **Startup Configuration** or **Backup Configuration**.
4	From the **Backup To** list, select the type of protocol you use to transfer the files.
5	In the **Server IP Address** field, type the IP address.
6	In the **FTP User Name** field, type the user name if the protocol is FTP.
7	In the **FTP Password** field, type the password if the protocol is FTP.
8	In the **File Name** field, type the name of the backup file.
9	Click **Apply.**

End

Variable definitions

Use the data in the following table to create backup for configuration files.

Variable	Value
Startup Configuration / Backup configuration	Specifies the configuration options. Select startup configuration to start the configuration. Select backup configuration to back up the configuration.
Backup To	Specifies the type of protocol you use to transfer the files. Select one of the following options. • TFTP • FTP The default value is TFTP.
Server IP Address	Specifies the server IP address.
FTP User Name	Specifies the FTP user name, if you select FTP.
FTP Password	Specifies the FTP password, if you select FTP.
File Name	Specifies the backup file name.

Restoring the BSG

- Restoring from a backup file (page 120)
- Restoring factory defaults (page 121)

Restoring from a backup file

Use the following procedure to restore the configuration of a BSG system by using the configuration information in a backup file stored on a remote computer. If the backup file is stored on a remote computer, the BSG automatically copies the backup file to the flash memory on the BSG system before beginning the restore operation. You must reboot the system to complete the restore operation.

Procedure steps

1. From the BSG navigation panel, select **Administration, Configuration File.**
2. Click **Restore.**

   The Restore Configuration dialog box appears.
3. From the **Restore From** list, select the type of protocol you use to transfer the files.
4. In the **Remote IP Address** field, type the remote IP address.
5. In the **FTP User Name** field, type the user name if the protocol is FTP.
6. In the **FTP Password** field, type the password if the protocol is FTP.
7. In the **File Name** field, type the file name.

8 Click **Apply**.

End

Variable definitions

Use the data in the following table to configure the fields in the restore configuration dialog box.

Variable	Value
Remote From	Specifies the type of protocol you use to transfer the files. Select one of the following options. • TFTP • FTP The default value is TFTP.
Remote IP Address	Specifies the remote IP address.
FTP User Name	Specifies the FTP user name, if you select FTP.
FTP Password	Specifies the FTP password, if you select FTP.
File Name	Specifies the file name.

Restoring factory defaults

Use the following procedure to reset the system to factory defaults. When you restore factory defaults, any configuration data saved in flash memory is lost. To save your configuration data, create a backup file before you reset the system to factory defaults. See Backing up configuration files (page 119) for more information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, Reset.** The Reset with factory default settings dialog box appears.
2	Click **Reset.**

End

BSG software upgrades

You can apply software updates to the BSG unit to introduce new functionality. Between software upgrades, you may find it necessary to apply software updates to resolve field issues.

Upgrading the BSG software

The following procedure describes how to update the BSG software using the Web user interface (UI).

Before you begin, ensure that the software update file is located in the root directory of the server. You can find software updates at:

http://www.nortel.com/support

Procedure steps

Step	Action
1	From the BSG navigation pane, select **Administration, Software Upgrade.** The Software Upgrade dialog box appears.
2	From the **Upgrade From** list, select the type of protocol you use to transfer the files. • If you select HTTP, a new window displays. Click **Browse** to select the file, and click **Upgrade**. • If you select FTP or TFTP, proceed to step 3.
3	In the **Server IP Address** field, type the IP address.
4	In the **FTP User Name** field, type the FTP user name if the protocol is FTP.
5	In the **FTP Password** field, type the FTP password if the protocol is FTP.
6	In the **File Name** field, type the software upgrade file name.
7	Click **Apply**.

End

Caution: Software upgrade erases the flash drive and takes few minutes to complete. To avoid damage to the flash drive, do not disturb the router during the upgrade.

Variable definitions

Use the data in the following table to use the Software Upgrade dialog box.

Variable	Value
Upgrade From	Specifies the type of protocol. Select one of the following options. • TFTP • FTP • HTTP The default value is TFTP.
Server IP Address	Specifies the Server IP Address.
FTP User Name	Specifies the user name, if you select FTP.
FTP Password	Specifies the password, if you select FTP.
File Name	Specifies the software file name to use for the upgrade. When the Upgrade From is HTTP, use the browse buton in the new pop-up window to select the file name.

Viewing system information

This chapter describes how to view information about the BSG system. You can use the Web UI to view general information, such as software and hardware version numbers. You can also view more detailed information, such as NAT translations and DHCP bindings, which is useful for debugging or troubleshooting the system.

Navigation

- Viewing the system summary (page 125)
- Viewing system files (page 126)
- Viewing PoE information (page 127)
- Viewing the IP interfaces (page 127)
- Viewing the Interface status (page 128)
- Viewing the DHCP bindings (page 129)
- Viewing the ARP cache (page 130)
- Viewing the MAC address table (page 130)
- Viewing the WLAN stations (page 131)

Viewing the system summary

Perform the following procedure to view BSG system information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.** The System Information dialog box appears.
2	View the details.

End

Variable definitions

Use the data in the following table to view the system summary.

Variable	Value
Switch Name	The name that identifies the switch.
Hardware Version	The hardware version of the hardware platform.

Variable	Value
Product Information	Information about the product. The information includes the following: Serial Number Manufacture Date Product Equipment Code PEC Release Number CPC Code System Hardware Installed Information
Software Version	The software version of the application.
Firmware Version	The version of the firmware that currently runs on the system.
SDK Version	The version of the software development kit (SDK).
RTE Version	The version of the run time environment (RTE).
SafeNet BOOTROM Version	The version of the SafeNet BOOTROM you use in the device.
SafeNet Firmware Version	The version of the SafeNet firmware you use in the device.
Wifi Firmware Version	The firmware version of the WiFi application that runs in the device.
Recommended VoIP BooTROM Version	The version of the recommended VoIP application BOOTROM.
VoIP Firmware Version	The version of the firmware of the VoIP application firmware.
Running Pack	The running pack.
Select Pack on Next Reboot	The pack for the next reboot. Options: • Pack1 • Pack2
Build Date	The build date of the application.
Logging option	The log option in use.
Logging Authentication Mode	The authentication mode of the log type.
Device Contact	The name of the person who manages the device.
Device Location	The physical location of the device.
Device Up Time	Time BSG runs.
Configuration Save Status	The save status of the system configuration.
Remote Save Status	The save status of the remote server connected to BSG.
Configuration Restore Status	The restore status of the system configuration.

Viewing system files

Perform the following procedure to view BSG system files.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, File Transfer, System Files.**

The System Files dialog box appears.

2 View the details.

End

Viewing PoE information

Perform the following procedure to view information about Power over Ethernet (PoE) in the BSG12 system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, Port Management, PoE Management.** The Global Power Management dialog box appears.
2	View the details.

End

Variable definitions

Use the data in the following table to view PoE information.

Variable	Value
Total PoE Power	The total PoE power available in Watts.
PoE Power Consumption	The current level of PoE power consumption.

Viewing the IP interfaces

Perform the following procedure to view the IP interfaces.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **IP Interfaces.** The IP Interfaces dialog box appears.
3	View the details.

End

Variable definitions

The following table describes the variables that appear on the IP Interfaces page.

Variable	Value
IP Interface	The name of the IP interface.
IP Address	The IP address assigned to the IP interface.
Subnet Mask	The netmask associated with the IP address.
Broadcast Address	The network address used for sending broadcast messages.
IP Assignment	The IP assignment mode of the interface. Options: Dynamic—external agent assigns the IP address. Static—user assigns the IP address.
Network type	The network type. Options: Local Area Network (LAN) Wide Area Network (WAN)
Link type	The network access type. Options: Private—for LAN. Public—for WAN.
Nat Status	The NAT status. Options: Enabled—for WAN interface. Disabled—for LAN interface.
Firewall Status	The firewall status. Options: Enabled—default for WAN interface. Disabled—default for LAN interface.
Interface Status	The current status of the interface. Options: UP DOWN

Viewing the Interface status

Perform the following procedure to view the interface status.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **Interface Status** located at the bottom of the page. The Interface Status dialog box appears.

3 Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the Interface Status page.

Variable	Value
Alias Name	An alias name for the interface. The network manager specifies the name. The name provides a non-volatile handle for the interface.
Description	The description about the interface. It also tells about the status of the interface, whether the status is up or down.
Administration Status	Desired state of the interface.
Operational Status	The current operational state of the interface.

Viewing the DHCP bindings

Perform the following procedure to view the Dynamic Host Configuration Protocol (DHCP) bindings. Use this procedure to see how many IP addresses have been assigned, the MAC address that the IP address has been assigned to, and how long the lease is for.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **DHCP Bindings** located at the bottom of the page. The DHCP Server Binding Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the DHCP Server Binding status information.

Variable	Value
IP Address	The IP address associated with the binding.
Hardware Address	The hardware address of the binding. The value is zero for the client identifier.

Variable	Value
Expiry Time(secs)	The remaining time for the binding, in seconds. Expired binding has negative value.
Binding State	The binding state. Options: Offered—the server sends the offer and waits for client's request. Assigned—the server assigns the address to the client. Probing—the DHCP server probes the address.

Viewing the ARP cache

Perform the following procedure to view the Address Resolution Protocol (ARP) cache. Use this procedure when you want to view the mappings between MAC and IP addresses connected to the BSG in the LAN or WAN.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **ARP Cache** located at the bottom of the page. The ARP Cache dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the ARP Cache page.

Variable	Value
Interface	The interface from which the entry was learned.
MAC Address	The MAC address which sent the ARP packet.
IP Address	The IP address of the host which sent the ARP packet.
Media Type	The ARP entry type. Options: Dynamic—learn dynamically. Static—configure statically.

Viewing the MAC address table

Perform the following procedure to view the Media Access Address (MAC) address table. You can use this procedure to see which address is routable through which port.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **MAC Address Table** located at the bottom of the page. The MAC Address Table dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the MAC Address Table page.

Variable	Value
VLAN ID	The VLAN ID for which you get filtering database information.
MAC Address	The MAC address for which the VLAN mapping exists in the entry.
Port	The port type to which the host with the MAC address is connected.
Status	The configuring status of the FDB entry. The status can be manual or static. Options: Learned or Management.

Viewing the WLAN stations

Perform the following procedure to view the Wireless Local Area Network (WLAN) access points in your network..

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.**
2	Click **WLAN Stations** located at the bottom of the page. The WLAN Station Statistics dialog box appears.
3	Click **Refresh.**

End

Variable definitions

The following table describes the variables that appear on the WLAN Station information page.

Variable	Value
Station Address	The MAC address that identifies the stations on the BSG.
SSID	The SSID with which the station is associated.

Variable	Value
Vlan ID	The VLAN ID with which traffic received on the SSID will be tagged.
Authentication status	The status of the authentication.
Association status	The associating status of the station.
Authorization status	The authorization status of the WLAN.
Association ID	The association ID of the station.
Authentication Type	The type of authentication. Options: open shared wpa wpa2 wpawpa2mixed wpapsk wpa2psk wpawpa2pskmixed open1x
Encryption Type	The type of encryption the station uses. Options: staticwep dynamicwep nokey aes tkip aestkip aeswep tkipwep aestkipwep
Radio Type	The type of radio. This field is available on the BSG12ew only.
Associated Time	The associated time. This field is available on the BSG12ew only.
Last Associated Time	The last associated time.This field is available on the BSG12ew only.
Last Disassociated Time	The last disassociated time. This field is available on the BSG12ew only.
Last 1x Authentication Time	The time of the last 1x authentication. This field is available on the BSG12ew only.
Last 802.11 Authenticated time	The time of the last 802.11 authentication. This field is available on the BSG12ew only.
Transmitted Bytes	The number of bytes per station transmits.
Received Bytes	The number of bytes per station receives.
Transmitted Packets	The number of packets per station transmits.
Received Packets	The number of packets per station receives..

Common operating procedures

This chapter provides information about procedures that you may use frequently in the normal operation of your network.

Navigation

- Saving configuration files (page 133)
- Updating system information (page 133)
- Configuring the date and time (page 135)
- Rebooting the system (page 136)
- Downloading files to the BSG (page 137)
- Uploading files from the BSG (page 138)

Saving configuration files

Use the following procedure to save the system configuration files in flash memory.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, Configuration File.** The Flash Save dialog box appears.
2	Click **Apply.**

End

Updating system information

Perform the following procedure to view BSG system information.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **System Summary.** The System Information dialog box appears.
2	In the **Switch Name** field, type the name for the BSG device.
3	In the **Device Contact** field, type the name of a contact person for this device.
4	In the **Device Location** field, type the location of the device.
5	Click **Apply.**

End

Variable definitions

Use the data in the following table to view the system summary..

Variable	Value
Switch Name	The name that identifies the switch.
Hardware Version	The hardware version of the hardware platform.
Product Information	Information about the product. The information includes the following: Serial Number Manufacture Date Product Equipment Code PEC Release Number CPC Code System Hardware Installed Information
Software Version	The software version of the application.
Firmware Version	The version of the firmware that currently runs on the system.
SDK Version	The version of the software development kit (SDK).
RTE Version	The version of the run time environment (RTE).
SafeNet BOOTROM Version	The version of the SafeNet BOOTROM you use in the device.
SafeNet Firmware Version	The version of the SafeNet firmware you use in the device.
Wifi Firmware Version	The firmware version of the WiFi application that runs in the device.
Recommended VoIP BooTROM Version	The version of the recommended VoIP application BOOTROM.
VoIP Firmware Version	The version of the firmware of the VoIP application firmware.
Running Pack	The running pack.
Select Pack on Next Reboot	The pack for the next reboot. Options: • Pack1 • Pack2
Build Date	The build date of the application.
Logging option	The log option in use.
Logging Authentication Mode	The authentication mode of the log type.
Device Contact	The name of the person who manages the device.
Device Location	The physical location of the device.
Device Up Time	Time BSG runs.

Variable	Value
Configuration Save Status	The save status of the system configuration.
Remote Save Status	The save status of the remote server connected to BSG.
Configuration Restore Status	The restore status of the system configuration.

Configuring the date and time

Perform the following procedure to configure the date and time for BSG system.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, System, Date and Time Settings.** The Date and Time Settings dialog box appears.
2	To set the time, select the **Set Time** check box.
3	Select a method for setting the date and time: **Manual** or **Time Server IP**.
4	If you selected **Manual**, enter the date and time settings.
5	If you selected **Time Server IP**, complete the following fields: • In the **Time Server IP** field, type the time server IP address. • In the **In Use IP** field, type the IP address that is in use.
6	In the **Poll Interval** field, enter an interval.
7	From the **Set Time Zone** list, select the time zone for your region.
8	From the **Synchronize Now** list, select whether to synchronize now or later.
9	From the **SNTP Client Status** list, select enabled or disabled.
10	To enable authentication, select the **Authentication** check box.
11	In the **Authentication Key-ID** field, type the authentication key ID.
12	In the **Authentication Key** field, type the authentication key.
13	To enable daylight savings, select the **Day Light Saving Time (DST)** check box.
14	To specify the start date for daylight savings time, in the **From** fields, select the **Day, Week**, and **Month**.
15	To specify the end date for daylight savings time, in the **To** fields, select the **Day, Week,** and **Month**.
16	Click **Apply.**

End

Variable definitions

Use the data in the following table to set the date and time for the system.

Variable	Value
Current Time	Specifies the current time.
Set Time	Select the Set Time check box to activate the options for setting the time: Manual, or Time Server IP.
Manual	To manually configure the time, select the Manual option and select values of the following fields: Date—Value range from 1 to 30. Month—month name from Jan to Dec. Year—Value range from 1 to 12. Hour—Value range from 0 to 23. Min—Value range from 0 to 59. Sec—Value range from 0 to 59.
Time Server IP	Specifies the time server IP address. Simple Network Time Protocol (SNTP) client connects to the SNTP server and sends an SNTP query message. Based on the response, the SNTP client updates the Co-ordinate Universal Time (UTC) or Greenwich Mean Time (GMT) accordingly.
Poll Interval	Specifies the polling interval. The range is from 4 to 14 seconds.
In Use IP	Specifies the IP address that is in use.
Set Time Zone	Specifies the time zone of your region.
Synchronize Now	Specifies whether to synchronize now or later. Select from the following options. • No • Yes
SNMP Client Status	Specifies the SNMP client status as enabled or disabled.
Authentication	Specifies whether authentication is enabled.
Authentication Key-ID	The authentication key ID for SNTP authentication. Enter this ID if you enabled Authentication. The value is from 0 to 65535.
Authentication Key	Specifies the authentication key, if authentication is enabled.
Day Light Saving Time (DST)	Specifies whether daylight saving time is enabled.
From	Specifies the day, week, month, and time to start daylight savings time.
To	Specifies the day, week, month, and time till when you want to disable DST.

Rebooting the system

Use the following procedure to reboot the system for new configuration settings to take effect.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, Reboot.**

The Rebooting the System dialog box appears.

2 Click **Reboot.**

3 Wait 5 minutes for the reboot to complete.

End

Downloading files to the BSG

Use the following procedure to download files to the BSG from another location in the network.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, File Transfer, File Download.** The File Download dialog box appears.
2	Select the type of file to download: **Digital Certicate**, or **Others**.
3	Select the protocol to use from the **Transfer Protocol** drop-down menu.
4	In the **Server IP Address** field, enter the IP address of the server to download the file from.
5	If you selected FTP as the transfer protocol, enter the user name in the **FTP User Name** field.
6	If you selected FTP as the transfer protocol, enter the password in the **FTP Password** field.
7	Click **Apply.**

End

Variable definitions

Use the data in the following table to download files to the BSG.

Variable	Value
Digital Certificate	Select this option to download a digital certicate.
Others	Select this option to download other types of files.
Transfer Protocol	Select the transfer protocol to use: TFTP or FTP.
Server IP Address	The IP address of the server to download from.
FTP User Name	If the transfer protocol is FTP, specify the FTP user name.
FTP Password	If the transfer protocol is FTP, specify the FTP password.
File Name	The name of the file to download. For digital certificates, the default name is sslservert.

Uploading files from the BSG

Use the following procedure to upload files from the BSG to another location in the network.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Administration, File Transfer, File Upload.** The File Upload dialog box appears.
2	Select the type of file to download: **Digital Certicate**, or **Others**.
3	Select the protocol to use from the **Transfer Protocol** drop-down menu.
4	In the **Server IP Address** field, enter the IP address of the server to upload the file to.
5	If you selected FTP as the transfer protocol, enter the user name in the **FTP User Name** field.
6	If you selected FTP as the transfer protocol, enter the password in the **FTP Password** field
7	Click **Apply.**

End

Variable definitions

Use the data in the following table to upload files from the BSG to another network location.

Variable	Value
Digital Certificate	Select this option to upload a digital certicate.
Others	Select this option to upload other types of files.
Transfer Protocol	Select the transfer protocol to use: TFTP or FTP.
Server IP Address	The IP address of the server to download from.
FTP User Name	If the transfer protocol is FTP, specify the FTP user name.
FTP Password	If the transfer protocol is FTP, specify the FTP password.
File Name	The name of the file to upload. For digital certificates, the default name is sslservert.

Initial troubleshooting

This chapter describes the initial steps to follow when you need to troubleshoot the BSG system.

Navigation

- Network configuration (page 139)
- Normal behavior on your network (page 140)
- Useful troubleshooting links (page 140)
- Diagnostic tools (page 142)

Network configuration

To keep track of your network's configuration, gather the information described in the following sections. This information, when kept up-to-date, is extremely helpful when you experience network or device problems.

- Site network map (page 139)
- Logical connections (page 139)
- Device configuration information (page 139)
- Other important data about your network (page 140)

Site network map

A site network map identifies where each device is physically located on your site, which helps locate the users and applications that are affected by a problem. You can use the site network map to systematically search each part of your network for problems.

Logical connections

With virtual LANs (VLANs), you must know how your devices are connected logically as well as physically.

Device configuration information

You should maintain online and paper copies of your device configuration information. Ensure that all online data is stored with your site's regular data backup. If your site does not have a backup system, copy the information onto a backup disk (such as a CD or zip disk) and store the backup disk at an offsite location.

Other important data about your network

For a complete picture of your network, have the following information available:

- **All passwords**—Store passwords in a safe place. It is a good practice to keep records of your previous passwords in case you must restore a device to a previous software version and need to use the old password that was valid for that version.
- **Device inventory**—It is a good practice to maintain a device inventory, which list all devices and relevant information for your network. The inventory allows you to easily see the device type, IP address, ports, MAC addresses, and attached devices.
- **MAC address-to-port number list**—If your hubs or switches are not managed, you must keep a list of the MAC addresses that correlate to the ports on your hubs and switches.
- **Change control**—Maintain a change control system for all critical systems. Permanently store change control records.
- **Contact details**—It is a good practice to store the details of all support contracts, support numbers, engineer details, and telephone and fax numbers. Having this information available when troubleshooting can save a lot to time.

Normal behavior on your network

When you are familiar with the performance of your network when it is fully operational, you can be more effective at troubleshooting problems that arise. To understand the normal behavior of you network, monitor your network over a long period of time. During this time you can see a pattern in the traffic flow, such as which devices are typically accessed or when peak usage times occur.

To identify problems, you can use a baseline analysis, which is an important indicator of overall network health. A baseline serves as a useful reference of network traffic during normal operation, which you can then compare to captured network traffic while you troubleshoot network problems. A baseline analysis speeds the process of isolating network problems. By running tests on a healthy network, you compile normal data for your network. This normal data can then be used to compare against the results that you get when your network is experiencing trouble. For example, ping each node to discover how long it typically takes to receive a response from devices on your network. Capture and save each device's response time and when you are troubleshooting you can use these baseline response times to help you troubleshoot.

Useful troubleshooting links

As part of your initial troubleshooting, Nortel recommends that you check these resources for information about known issues and for solutions related to the problem you are experiencing.

Navigation

- Partner Bulletins (page 141)
- Knowledge and Solution Engine (page 141)

Partner Bulletins

To locate Partner Bulletins, visit the Nortel Partner Information Center:

http://www.nortel.com/pic

Knowledge and Solution Engine

The Knowledge and Solution Engine allows you to search an entire database of Nortel technical documents, troubleshooting solutions, software, and technical bulletins.

The document types available from the Knowledge and Solution Engine include the following:

- Bulletins: Includes a listing of technical bulletins.
- Documentation: Includes all technical documentation written for Nortel
- products (such as installation guides, administration guides, release
- notes).
- Service Requests: Includes technical support cases created within the past year. The availability of service requests is based on your customer entitlement.
- Software: Includes software patches and software releases.
- Solutions: Includes troubleshooting solutions written by the Nortel Technical Support team.

When searching through the Knowledge and Solution Engine, enter a natural language query (that is, a query in the form of a statement or a question).

Using the Knowledge and Solution Engine

Use the following procedure to access the Knowledge and Solution Engine.

To use the Knowledge and Solution Engine

1. Go to the Nortel Web site: **www.nortel.com**
2. Log in using user name and password.
3. Select **SUPPORT & TRAINING**.
4. Select **ONLINE SELF-SERVICE**, and then select **Knowledge Base**.

   The Online Self-Service page appears and shows the Knowledge and Solution Engine. For information on performing your search, click the **Search Tips** link.

   To view an interactive tutorial for the Knowledge and Solution Engine, go to the **Help & Contact** section, click the **Help Using This Site** link and then scroll to find the **Knowledge Base** tutorial.
5. Enter your problem statement or question in the text box. Ensure that you leave spaces between the words in the statement or question.

6 From the **ALL TYPES** drop-down list, select the document type you would like to search against. The default is ALL TYPES, which searches on all available documents (bulletins, documentation, services requests, software, and solutions).

7 Click **>** (the arrow adjacent to the text box) or press **Enter** to start your search. The page reloads and provides the option to narrow your search by product family.

Diagnostic tools

The BSG offers diagnostic tools to help you troubleshoot problems in your network:

- Ping (page 142)
- SIP diagnostics (page 142)
- T1/E1 loopbacks (page 143)

Ping

Ping (Packet InterNet Groper) is a utility that you can use to verify that a route exists between the BCM and another device. Use this procedure to verify connectivity between the BSG and another device,

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Device Monitoring, Diagnostic Tools**.
2	In the **Destination IP Address** field, enter the IP address of the device that you wish to ping.
3	Click **Apply**. The results display in the **Ping Response** window.

Variable definitions

Use the data in the following table to use the fields in the Ping Settings page.

Variable	Value
Destination IP Address	Specifies the IP address of the device for which you want to verify connectivity.

SIP diagnostics

You can use SIP diagnostics to enable call traces, detailed trace logging, and brief trace logging.

Procedure steps

Step	Action
1	From the BSG navigation panel, select **Configuration, SIP, System Configuration, Diagnostics** tab.
2	In the Dump SIP Messages drop-down menu, select Enable or Disable.
3	Under Detailed Traces, select the radio button that corresponds to the level of detailed trace: All, None, or Selected.
4	If you chose Selected, click the checkboxes to enable specific traces.
5	Under Brief Traces, select the radio button that corresponds to the level of detailed trace: All, None, or Selected.
6	If you chose Selected, click the checkboxes to enable specific traces.
7	Click **Apply**.

Variable definitions

Use the data in the following table to use the fields in the SIP Diagnostics page.

Variable	Value
Dump SIP Messages	Specifies the status of call traces. Options: Enable—enable call traces. Disable—disable call traces. The default value is Disable.
Detailed Traces	Specifies the type of detailed trace: All—log all traces. None—log no traces. Selected—log traces for the selected value(s). Select any of the following traces: Call Server, Registrar, ALG-CAC, Routing Engine, and Carrier Monitoring. The default value is All.
Brief Traces	Specifies the type of brief trace: All—log all traces. None—log no traces. Selected— log traces for the selected value(s). Select any of the following traces: Call Server, Registrar, ALG-CAC, Routing Engine, and Carrier Monitoring. The default value is None.

T1/E1 loopbacks

Use the following procedure to test transmission on the T1/E1 link on the BSG12tw.

Procedure steps

Step	Action

1. From the BSG navigation panel, select **Device Monitoring, Diagnostic Tools, T1/E1**.
2. From the **Interface** list, select the T1/E1 interface on which you want to perform a loopback.
3. From the **Loop Back Configuration** list, select the type of loopback to apply.
4. Click **Apply**.

Variable definitions

Use the data in the following table to use the fields in the T1/E1 Diagnostics page.

Variable	Value
Interface	The T1/E1 interface on which to perform the loopback.
Loop Back Configuration	The type of loopback. The options are: • No Loopback • Payload Loopback—The received signal is looped back for retransmission after it has passed through the framing function of the BSG. • Line Loopback—The data is looped back through the LIU. • Inward Loopback—The transmitted signal at the interface is looped back and received by the same interface (local loopback). • Dual Loopback—Both Line Loopback and Inward Loopback are active.

Advanced troubleshooting on the BSG

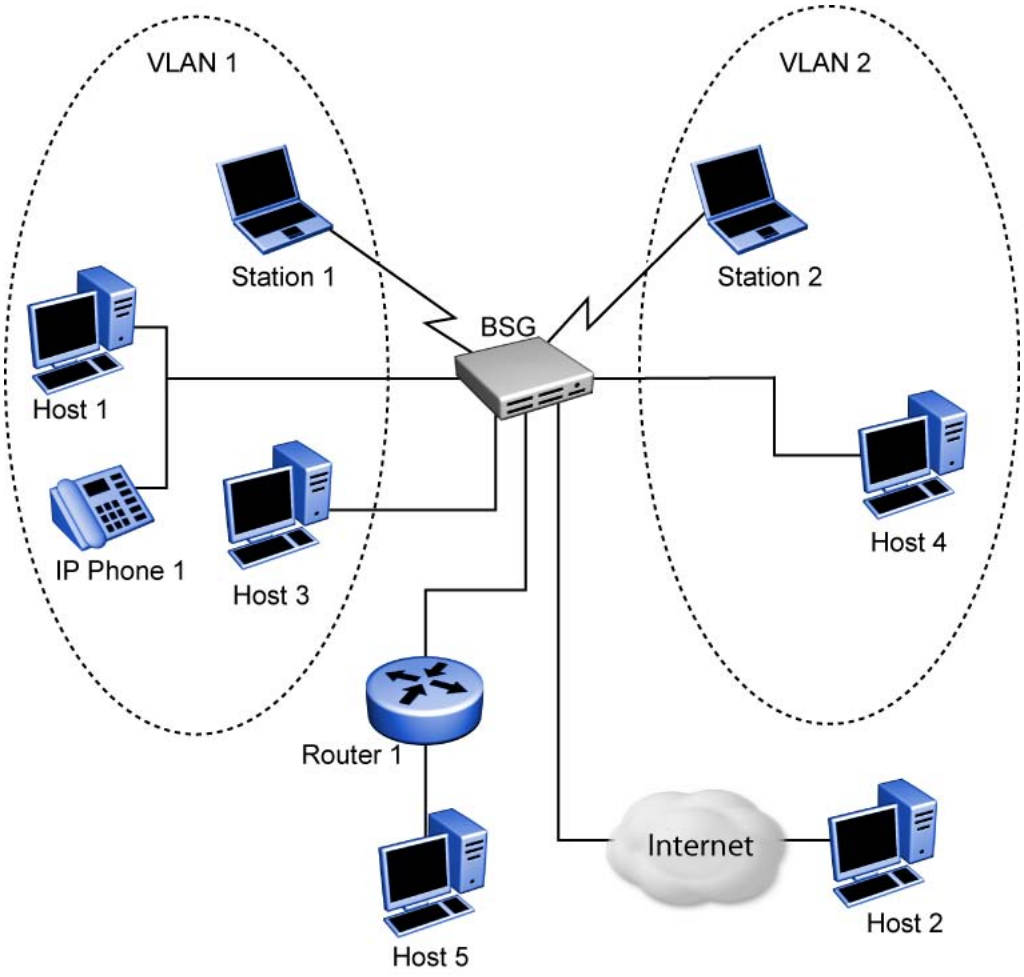
This chapter describes problems that may occur in your network, and how to troubleshoot them.

Navigation

- Switching and routing (page 146)
- WAN and VPN (page 149)
- Telnet (page 154)
- BSG subsystem (page 157)
- Firmware upgrade (page 166)

The following figure shows the network topology used in these sample scenarios.

Figure 2 Sample topology for troubleshooting



Switching and routing

This section describes troubleshooting scenarios related to switching and routing functionality.

Navigation

- Layer 2 switching is not functioning (page 147)
- Layer 3 forwarding is not functioning (page 148)
- LAN host does not receive an automatic IP address (page 148)

Layer 2 switching is not functioning

Use the following procedure when both computers are on the same VLAN, but cannot communicate. In Figure 2 on page 146, this scenario would exist when Host 1 is unable to reach Host 3.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to verify current status of the interface. `show interfaces [<interface-type> <interface-id>] etherchannel`
5	Execute the following command to ensure the administration status is up. `no shutdown port-channel`
6	Verify whether the cable that connects the host and the BSG router is properly connected to ensure the operation status is up.
7	Execute the following command to verify if spanning tree is **enabled** and if the port state is **forwarding**. `show spanning-tree interface <interface-type> <interface-id> [{cost | priority | portfast | rootcost | state | stats | detail}]`
8	Wait 30 seconds for the port to become forwarding, or execute the command to make it an edge port. `show spanning-tree [{summary | blockedports | pathcost method }]`
9	Execute the following command to ensure that the MAC address of the destination host is learned on the port. `show mac-address`
10	If the MAC address of the host is learned on the incorrect port, then initiate traffic from the host to another host or wait for the flush-out time of the MAC address table.
11	Verify the VLAN port configuration.
12	Execute the following command to verify whether the ports are marked as untagged ports. `show vlan [brief | id <vlan-id(1-4094)> | summary]`
13	Execute the following command to verify if the switch Port Vlan ID (PVID) configuration is correct. `show vlan port config [port <interface-type> <interface-id>]`

End

Layer 3 forwarding is not functioning

Use the following procedure if Layer 3 forwarding is not functioning; that is, if forwarding out of the VLAN is not working. In Figure 2 on page 146, this scenario would exist when Host 1 is unable to reach Host 5.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Verify whether the IP address configurations are correct and are configured in the correct subnet in the router and in the hosts.
5	Verify whether all the interfaces (physical or virtual) are administratively and operationally up using the following command: `show ip interface`
6	Verify whether the routing table is updated properly and has routes for the network using the following command: `show ip route`
7	Execute the following command to verify whether ARP is running and whether the IP address to MAC address mapping is successful. `show ip arp [{Vlan <vlan-id(1-4094)> | <ip-address> | <mac-address> | summary | information}]`

End

LAN host does not receive an automatic IP address

Use the following procedure if a LAN host does not receive an IP address; that is, Host 1 does not receive an IP address from the BSG.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to ensure that DHCP server is running on the network and that the DHCP server status is enabled. `show ip dhcp server information`
5	Execute the following command to ensure that an IP address pool is available in the server for the client subnet. `show ip dhcp server pools`

6 Execute the following command to ensure connectivity between the server and the client.

```
show interface description
```

7 Execute the following command to enable trace messages in both the DHCP server and the client.

```
debug ip dhcp server {all | events | packets | errors | bind}
```

8 Ensure that DHCP packets are sent from the client and that the same are received at the server.

End

Attention: If BSG operates as a DHCP client while it is connected to a third-party DHCP server, ensure that the DHCP server is running and enabled and that the DHCP address pool is available on the server.

Also, verify if connectivity between the server and client exists. Execute the debug ip dhcp server command to enable trace messages in both the DHCP server and the client. Verify that the DHCP packets are sent from the client and the same are received at the server.

WAN and VPN

This section describes troubleshooting scenarios related to Wide Area Network (WAN) and Virtual Private Network (VPN) functionality.

Navigation

- WAN access failure (page 149)
- Firewall issues (page 150)
- No traffic between WAN and LAN host (page 151)
- Verifying site-to-site VPN connectivity (page 152)
- DNS does not resolve the domain name (page 152)
- PPP link does not start (page 153)

WAN access failure

Use the following procedure if WAN access is not working and there is no connectivity. In Figure 2 on page 146, this scenario would exist when Host 1 is unable to reach Host 2.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.

3 In the **Password** prompt, type the password.

4 To access services on the Internet, the WAN interface of BSG needs a valid IP address. If you use a DHCP client on a WAN interface to obtain the IP address from your ISP, verify whether the DHCP address assignment was successful.

5 Execute the following CLI commands to verify the IP address of WAN interface. The address should not be 0.0.0.0.

```
show interface description
show ip interface
```

6 Execute the following command to verify whether a default route exists to reach the Internet.

```
show ip route
```

End

Firewall issues

When you have connectivity and the WAN interface has an IP address, but you cannot reach all parts of the network, you may have a firewall configuration problem. Use the following procedure to solve firewall-related problems.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	By default, firewall and NAT are automatically enabled on the WAN interface. Ensure that there are firewall filters and ACLs are set up to allow Internet traffic, typically DNS and HTTP.

5	Execute the following CLI commands to verify whether firewall filters and access lists for the filters are available to permit Internet traffic.
	`show firewall filters`
	`show firewall access-lists`

6	Execute the following command to verify DNS settings. Verify that DNS forwarder is enabled and configured with the correct IP address of the DNS server. `show dns listRR`

7	Execute the following commands to know whether packets are dropped by the firewall.
	`show firewall stats`
	`show firewall logs`

End

No traffic between WAN and LAN host

Use the following procedure if the traffic between WAN and LAN host is not successful; that is, the traffic from Host 1 to Host 2 exists, but does not flow from Host 2 to Host 1.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to ensure that LAN and WAN interfaces are up. `show ip interface`
5	Verify whether the IP address configurations are correct and are configured in the correct subnet on the router and on the LAN host.
6	Execute the following command to verify that the firewall filters are configured to allow incoming traffic from WAN. `show firewall filters`

7	If filters are not configured, execute the following command to add a firewall filter based on IP address range, protocol, and port. You must be in firewall configuration mode to add the filters.
	`filter add <filter name> {src ip/range|any} {dest ip/ range|any}`
	`[<tcp|udp|icmp|igmp|ggp|ip|egp|igp|nvp|rsvp|igrp|ospf|any> ] [srcport`
	`<range>] [destport <range>]`

8	Execute the following command to verify if Access Lists are created for the WAN interface. `show firewall access-lists`
9	If access lists are not configured, execute the following command to create an access rule for the WAN Interface. `access-list`

10	Execute thefollowing commands to ensure if NAT is configured for either the virtual server or the static NAT.
	`show virtual servers`
	`show ip nat static`

11	Execute the following command to configure virtual server. You must be in interface configuration mode to add a virtual server. `virtual server <local IP address> [<local port number>] {auth | dns | ftp | pop3 | pptp | telnet | http | nntp | snmp | other} [<global port number>]} } [<description>]`

12 Execute the following command to add a static mapping between local and global addresses on the specified interface. You must be in interface configuration mode to add a static mapping.

```
static nat <local IP address> <translated local IP address>
```

End

Verifying site-to-site VPN connectivity

Use the following procedure if the site-to-site VPN connectivity is not working.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to determine if the crypto parameters are configured correctly. `show crypto vpn map <policy name>`
5	Crypto parameters might have been configured but not applied to an interface. Execute the following command to apply the policy on an interface. You must be in interface configuration mode to execute this command. `crypto map <policy name>`
6	Send a ping to determine whether there is connectivity between the sites.

End

DNS does not resolve the domain name

Use the following procedure if the DNS is not resolving the domain name.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to verify the status of the DNS Server and the configured primary and secondary addresses. `show dns [listRR]`
5	Execute the following command to enable the DNS server if it is disabled. You must be in global configuration mode to enable the DNS server. `dns-server forwarder { enable | disable }`

6 Execute the following command to configure the primary or secondary or both IP addresses for dns-forwarder. You must be in global configuration mode to execute this command.

```
dns-server forwarder [primary <unicast_ip_addr>] [secondary <unicast_ip_addr>]
```

7 If DNS is not resolving IP address for a requested host (name) locally, the DNS tries to resolve it from primary server.

8 If the problem is not resolved by primary server, the DNS tries to resolve the problem from secondary server.

9 If the problem is not resolved by secondary server address, the request times out.

End

PPP link does not start

Use the following procedure if PPP link does not start.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to ensure that the PPP link is layered over the correct physical interface. `show interface ppp <index> config`
5	Execute the following command to verify if both the physical interface and the PPP interface are administratively up and that the physical interface is operationally up. `show interface description`
6	If the administration status is down, execute the following command from the interface configuration mode to ensure that the status is up. `no shutdown`
7	Execute the following command to configure the PPP logon name and password. `ppp username <user-name> password <password>`
8	Execute the following command to verify if **peer authentication** is enabled. `show interface ppp <index>`

9 If BSG is operating as PPPoE client, execute the following command to disable peer authentication. You must be in either PPP interface configuration mode, or multilink PPP interface configure mode to execute this command.

```
no ppp authenticate username
```

End

PPP link fails when the WAN interface is DSL

Use the following procedure if PPP link fails when DSL is used as the WAN interface.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to ensure that the PPP link is layered over the correct physical interface. `show interface ppp <index> config`
5	Execute the following command to verify if both the physical interface and the PPP interface are administratively up and that the physical interface is operationally up. `show interface description`
6	If the administration status is down, execute the following command from the interface configuration mode to ensure that the status is up. `no shutdown`
7	Execute the following command and verify that the PPP interface is able to obtain the IP Address of the PPoE server. `show ip interface`
8	Execute the following command to verify that the PVC is properly configured and whether DSL has negotiated the connection mode properly. `show dsl interface pvc <index>`

Telnet

This section describes troubleshooting scenarios related to Telnet functionality.

Navigation

- "Determining whether Telnet is operational" (page 155)
- "Verifying a Telnet session" (page 155)
- "Determining whether SSH connects" (page 156)

Determining whether Telnet is operational

Use the following procedure if Telnet is not operational.

Procedure steps

Step	Action
1	Log in to the BSG Web UI.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Ping the IP address of the host with which you cannot establish a Telnet session. If ping is successful verify if Telnet is enabled globally.
5	If ping is not successful, verify if the routing statement on BSG is correct and that it has an ARP entry for the default gateway using the following command. `show ip arp`
6	Verify if telnet is enabled on standard port (port 23).
7	Execute the following command to enable telnet at the host. You must be in global configuration mode to enable Telnet. `set ip telnet enable`
8	Verify for firewall filters and ACLs. Execute the following command with TCP, UDP, ICMP, and IGMP protocols enabled as Telnet operates on TCP traffic. You must be in firewall configuration mode to add a filter. `filter add <filter name> {src ip/range|any} [<tcp | udp | icmp | ggp | ip | egp |igp | nvp | rsvp | igrp | ospf | any>] [srcport <range>] [destport <range>]`

End

Attention: For WAN - LAN Connectivity

Execute the **show virtual servers** command to verify if Telnet is included in the application modes of the virtual server.

Execute the **virtual servers** command to include Telnet for the required configuration to take effect.

Attention: For LAN-WAN Connectivity

In case of LAN - WAN connectivity, firewall filters exist and therefore problems with Telnet might not occur.

Verifying a Telnet session

Use the following procedure if a Telnet session times out after it remains idle for a period of time.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to increase the inactivity time. You must be in line configuration mode to execute this command. `exec-timeout <integer (1-18000)>`
5	Execute the following command to clear the configured inactivity time and configure the default value. You must be in line configuration mode to execute this command. `no exec-timeout`
6	The use of this command differs depending on whether you connect to the target using console or Telnet.
7	If you connect the target from the console, execute the following set of commands. • `bsg#configure terminal` • `bsg(config)# line console` • `bsg(config)# no exec-timeout` • `bsg(config)# end` • `bsg# show line`
8	If you connect to the target using Telnet, execute the following set of commands. • `bsg# configure terminal` • `bsg(config)# line vty` • `bsg(config)# no exec-timeout` • `bsg(config)# end` • `bsg# show line`

End

Determining whether SSH connects

Use the following procedure if SSH does not connect.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.

4 Ping the IP address of the host.

5 If the ping is successful, execute the following command to verify if SSH is enabled globally on the device.

```
show ip ssh
```

6 If SSH is disabled, execute the following command to enable SSH on the device. You must be in global configuration mode to execute this command.

```
ip ssh {version compatibility | cipher ([des-cbc]) | auth
([hmac-md5] [hmac-sha1])}
```

7 Verify if SSH is enabled on the standard port (port 22).

8 Verify that the version compatibility of the host to be connected matches the version compatibility of the BSG.

9 Verify if the maximum number of SSH sessions (10) allowed is reached.

End

BSG subsystem

This section describes troubleshooting scenarios related to BSG subsystem functionality.

Navigation

- Determining whether VOIP/SafeNet/SIP/ Wireless is operational (page 157)
- Troubleshooting SIP (page 158)
- Troubleshooting WLAN (page 164)

Determining whether VOIP/SafeNet/SIP/ Wireless is operational

Use the following procedure if VoIP/SafeNet/SIP/ Wireless subsystem is not functional when the BSG is up.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to verify that each subsystem has the latest firmware version. `show sub-system information [ { wifi | voip | safenet | dsl}]`
5	By default, when the BSG is up, VLAN starts with the default VLAN 4093. Verify if VLAN 4093 is present.

6 Execute the following command to ensure that network is configured on VLAN 4093.

```
show ip interface Vlan 4093
```

- For BSG8, Port 8 is a member port for this VLAN. The administration and operation status of this VLAN must be up with the IP address 169.254.1.1.
- For BSG12 ,Ports 13, 14, 15 and 16 are member ports for this VLAN. The administration and the operation status of this VLAN must be up with the IP address 192.168.1.1.

7 Execute the following commands to verify the MAC and ARP entries of the subsystems.

- `show command`
- `show ip arp`
- `show mac-address-table`

8 Each subsystem is configured with a specific IP Address to communicate with VLAN 4093. Ping the corresponding IP address to ensure proper communication.

End

Troubleshooting SIP

This section descibes troubleshooting scenarios related to SIP functionality.

Navigation

- Determining whether SIP server is down (page 158)
- Verifying whether SIP server status is in BackupWanDown mode (page 159)
- Verifying whether SIP server status is in BackupWanUp mode (page 159)
- Executing SIP related CLI command (page 160)
- Verifying whether SIP messages reach the network (page 160)
- Getting a 503 error message for INVITE request (page 161)
- Getting 408, 500, or 504 responses for REGISTER request (page 162)
- Gettinga 405 response for REGISTER request (page 163)
- Getting 403 forbidden response for REGISTER request (page 163)

Determining whether SIP server is down

Use the following procedure if SIP server is down.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.

2 In the **Login** prompt, type the login name.

3 In the **Password** prompt, type the password.

4 Execute the following command to view the status of the SIP server. It must be operational.

```
show sipserver status
```

5 If the status of the SIP server is disabled, execute the following command to enable the SIP server. You must be in SIP configuration mode to execute this command.

```
sip {enable | disable}
```

End

Verifying whether SIP server status is in BackupWanDown mode

Use the following procedure if SIP server status shows BackupWanDown mode and the server is not moving to normal mode.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Ensure that the WAN link is connected.
5	Execute the following command to verify that the WAN link status is up and that has acquired IP address. `show interface description`
6	The status of Fa0/9 interface should be up.

End

Verifying whether SIP server status is in BackupWanUp mode

Use the following procedure if SIP server status shows BackupWanUp mode and the server is not moving to normal mode.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to view the carrier server details. `show sipserver PolledServers`

5 If carrier server details are not configured, execute the following command to configure the carrier server details. You must be in SIP domain configuration mode to execute this command.

```
set sipserver PolledServers Poliingaddress {ipaddress | hostname <hostname>}{port<1-65535>] [pollinterval <(10-600)seconds>] [pollretries <1-10>] [transport {tcp | udp | tls}]}
```

6 Ensure that BSG sends OPTIONS SIP message to the carrier server and that carrier server responds to this request with a response other than 408 and 503.

End

Executing SIP related CLI command

Use the following procedure if you receive a message when you execute any SIP-related CLI command that states the SIP module is disabled.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to enable the SIP module. You must be in SIP configuration mode to execute this command. `sip enable`

End

Verifying whether SIP messages reach the network

Use the following procedure if SIP messages sent by BSG do not reach the network.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Verify whether firewall rules are configured properly.
5	Execute the following commands to create firewall filter rules for BSG SIP server. • `bsg# configure terminal` • `bsg(config)# firewall`

- `bsg(config-firewall)# filter add f1 192.168.1.1/32 any any srcport >=1024`
- `bsg(config-firewall)# filter add f2 10.0.0.1/32 any any srcport <=4999`
- `bsg(config-firewall)# access-list acl1 out f1,f2 permit 1`

6 The IP address of VLAN 1 interface is 192.168.1.1.

7 If SIP related issues do not get resolved by the steps given above, please collect traces and provide the file (cas.log) for further analysis.

8 Execute the following commands for enabling SIP traces.

- `bsg(config)# logging trap 7`
- `bsg(config)# logging flash`
- `bsg(config-sip-traces)# set sipserver SIPMessageDumps False`
- `bsg(config-sip-traces)# set sipserver DetailedTraces All`
- `bsg(config-sip-traces)# set sipserver BriefTraces All`

End

Getting a 503 error message for INVITE request

Use the following procedure if phones registered with BSG receives a 503 service unavailable response for an INVITE request.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	If the Warning header contains, *370 CAS Insufficient Bandwidth,* execute the following command. `show sipserver MaximumSimWANCallsAllowed`
5	Verify whether WAN link interface name and maximum simultaneous calls to be allowed are configured.
6	Verify whether firewall rules are configured properly.
7	If maximum simultaneous calls is not configured, execute the following command in CLI to configure the maximum simultaneous calls. `set sipserver MaximumSimWANCallsAllowed {[<WAN1 link> <MaxCalls(1-500)>] [<WAN2 link> <MaxCalls(1-500)>] [<WAN3 link> <MaxCalls(1-500)>]}`
8	Execute the following command

```
bsg(config-sip-bsg)# set sipserver
MaximumSimWANCallsAllowed Fa0/9 20
```

Attention: WAN link name (Fa0/9) is case-sensitive.

9 If maximum simultaneous calls is configured properly, then verify that the current ongoing call count does not exceed the maximum simultaneous call count configured.

10 If the Warning header contains *399 Request addressed to public domain and WAN link is down,* verify whether the backup mode dial plan is correct and request does not addresses to public domain.

11 Execute the following command.

```
bsg(config-sip-traces)# set sipserver BriefTraces All
```

End

Getting 408, 500, or 504 responses for REGISTER request

Use the following procedure if phones registered with BSG receives 408, 500, or 504 response for a REGISTER request. The codes indicate the following problems:

- 408—Request Timeout
- 500—Server Internal Error
- 504—Server Timeout

Procedure steps

Step	Action
1	Verify the domain name configured in BSG, carrier server, and the phones. All should have the appropriate domain name configured.
2	Verify whether the configured dial plan is correct.
3	Verify whether request URL is sent with proper domain name.
4	Log in to the BSG CLI through Telnet or SSH.
5	In the **Login** prompt, type the login name.
6	In the **Password** prompt, type the password.
7	Execute the following command to view the domain name configured in BSG. `show sipserver serverdomainname`
8	Execute the following command to configure the domain name in BSG using CLI. You must be in SIP domain name configuration mode to execute this command. `set serverdomainname`

End

Gettinga 405 response for REGISTER request

Use the following procedure if phones registered with BSG receive a 405 response for a REGISTER request.

Procedure steps

Step	Action
1	Verify that the request URL in REGISTER contains the domain name and not the VLAN 1 address.

End

Getting 403 forbidden response for REGISTER request

Use the following procedure if phones registered with BSG receives a 403 forbidden response for REGISTER request.

Procedure steps

Step	Action
1	Verify whether the subscriber is provisioned in BSG if the dynamic subscription option is disabled.
2	Log in to the BSG CLI through Telnet or SSH.
3	In the **Login** prompt, type the login name.
4	In the **Password** prompt, type the password.
5	Execute the following command to view the status of dynamic subscription. `show sipserver AddDynamicSubscriber`
6	Execute the following command to enable dynamic subscription feature, which dynamically add a subscriber entry into the database on receiving a REGISTER request.You must be in SIP registration configuration mode to execute this command. `set sipserver AddDynamicSubscriber True`
7	If dynamic subscription is disabled, manually add a subscriber entry using the command. You must be in SIP configuration mode to execute this command. `add subscriber <user-name> <domain-name> [alias <alias-name>] [calling-line-identity <subscriber_identity>]`
8	Execute the following command to view the subscriber entries. `show sipserver subscriber details {all | <user-name> <domain-name>}}`

End

Attention: Ensure that the subscriber is provisioned in the carrier server.

Troubleshooting WLAN

This section descibes troubleshooting scenarios related to WLAN functionality.

Navigation

- Determining whether WLAN stations have access in LAN or WAN (page 164)
- Determining whether WLAN host receives IP address (page 165)
- Verifying for authentication (page 165)

Determining whether WLAN stations have access in LAN or WAN

Use the following procedure if WLAN stations cannot have access in LAN or WAN; that is, H1 is unable to reach STA1 / STA2.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command to verify if the radio is up. `show interface description`
5	If the radio administration status is down, execute the following commands to ensure the radio status is up. • `bsg(config)# interface radio 1/1` • `bsg(config-radio)# config dot11 enable network`
6	Execute the following command to verify if the interface status is up. `show interface description`
7	Execute the following command to verify whether the station is in authorized state.

Attention: On the wireless client side, verify whether the station is connected to the SSID.

	`show client ap global`
8	Verify whether the authentication keys (WEP and PSK) are the same in both the BSG and the client.
9	Reconfigure the keys if required. At the BSG, execute the following command to configure the keys. `config wlan security`
10	Verify whether the VLAN associated to the SSID is up.

11 Execute the following command to obtain the VLAN associated to the SSID.

```
show vlan
```

End

Determining whether WLAN host receives IP address

Use the following procedure if WLAN host does not receive an IP address.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.
3	In the **Password** prompt, type the password.
4	Execute the following command and receive the VLAN ID that is associated with the given WLAN ID. `show wlan [<Wlan-Id>]`
5	Execute the following command and receive the IP Address of the VLAN ID. `show ip interface`
6	Execute the following command to verify if an IP address pool is present for this network. `show ip dhcp server pools`
7	Execute the following command to create a DHCP Server address pool if the pool is not configured for the IP address of the VLAN. `ip dhcp pool <index (1-2147483647)>`
8	Execute the following command to enable the DHCP server. You must be in global configuration mode to execute this command. `service dhcp-server`
9	Execute the following command to create a DHCP Server address pool. You must be in global configuration mode to execute this command. `ip dhcp pool <index (1-2147483647)>`

End

Verifying for authentication

Use the following procedure if authentication is disabled on wireless ports.

Procedure steps

Step	Action
1	Log in to the BSG CLI through Telnet or SSH.
2	In the **Login** prompt, type the login name.

3 In the **Password** prompt, type the password.

4 Execute the following command to view Service Set IDentifier (SSID) settings and to determine whether security is configured for the SSID. You can configure security by using WEP and by using a pre shared key.

```
show wlan
```

5 For WEP, the security authentication type must be shared.

6 To configure security using WEP, execute the following command with the authentication type as shared. You must be in global configuration mode to execute this command.

```
config wlan security auth- type {open | shared | wpa | wpa2
| wpa-wpa2-mixed | wpa-psk | wpa2-psk | wpa-wpa2-psk-mixed
| open1x} <wlan-id(1-4)>
```

7 Execute the following command to configure static WEP keys and indexes. You must be in global configuration mode to execute this command.

```
config wlan security static-wep-key encryption
<wlan-id(1-16)> {64 | 128 | 152} {hex | ascii} <key>
<keyindex(1-4)>
```

8 Execute the following command to configure the WEP default key index of a particular SSID. You must be in global configuration mode to execute this command.

```
config wlan wep default-key <wlan-id(1-4)> <key-index(1-4)>
```

9 Configure the wireless device.

10 To configure security using a pre-shared key, execute the following command with the authentication type wpa2-psk. You must be in global configuration mode to execute this command.

```
config wlan security auth- type {open | shared | wpa | wpa2
| wpa-wpa2-mixed | wpa-psk | wpa2-psk | wpa-wpa2-psk-mixed
| open1x} <wlan-id(1-4)>
```

11 Execute the following command to configure the PSK value.

```
config wlan security pre-shared-key <wlan-id(1-16)> {hex |
ascii} <key>
```

End

Firmware upgrade

This section descibes the troubleshooting scenerio related to a firmware upgrade. Use the following procedure if you cannot upgrade to the latest version of firmware.

Procedure steps

Step	Action
1	Verify if the TFTP server on which the firmware is placed is operational.
2	Verify for PING connectivity between the TFTP server and the BSG.

3 Verify whether the LAN/WAN cables are properly connected.

4 Verify if the **.jffs2** file is in the specified directory of the TFTP server.

5 Verify if any other file is downloaded instead of the **.jffs2** file.

Attention: .Before you upgrade the Software Packs, verify the file type to be a true Linux binary file and a true Flash File System file.

6 Verify if partitions in the flash are configured properly and whether the size of the partitions does not exceed the allocated partition size.

Attention: If the TFTP server is on the WAN side, execute the enable command in firewall configuration mode. If necessary, enable the firewall. If the firewall is enabled but the upgrade still does not occur, then verify whether the firewall has the correctly configured rules to enable pass the tftp/ftp/http/sftp/scp data packets.

7 After the firmware upgrade, if the kernel panics while booting up, watchdog functionality resets the board. System starts with the older image automatically.

End